



ENCENTUATE®



Encentuate® Identity and Access Management (IAM)

Enterprise Deployment Guide

Product version 3.6

Document version 3.6.4

Copyright notice

Encentuate[®] IAM Enterprise Deployment Guide version 3.6.4

Copyright © March 2008 Encentuate[®]. All rights reserved.

The system described in this guide is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Any documentation that is made available by Encentuate is the copyrighted work of Encentuate and is owned by Encentuate.

NO WARRANTY: Any documentation made available to you is as is, and Encentuate makes not warranty of its accuracy or use. Any use of the documentation or the information contained herein is at the risk of the user.

Documentation may include technical or other inaccuracies or typographical errors. Encentuate reserves the right to make changes without prior notice.

No part of this document may be copied without the prior written approval of Encentuate.

Trademarks

Encentuate[®] is a registered trademark in United States of America, Singapore and United Kingdom. Transparent Crypto-Identity, IAM, Encentuate AccessAgent, AccessStudio, Encentuate USB Key and Wallet are trademarks of Encentuate[®]. All other trademarks are the property of their respective owners.

Contact information

For more information about this product or any support enquiries, contact us:

To log a support incident: <https://customercare.encentuate.com>

To reach us by phone:

- Americas: +1-800-ENCENTUATE ext 5 (+1-866-362-3688 ext 5)
- Asia Pacific: +65-6862-7085

Email: customercare@encentuate.com

Table of Contents

About This Guide	1
Purpose	1
Audience	1
What's in this guide	1
Document conventions	2

Part I: Introduction to Encentuate IAM Enterprise 6

About Encentuate IAM Enterprise	7
Encentuate IAM Enterprise features	7
System overview	10
Encentuate product components	10
User roles	11
Policies	12
Using Wallets	14
Minimum system requirements	15
Supported servers	15
Hardware requirements (not including database)	15
Network requirements	16
IMS Server software requirements	16
Roaming support matrix	16
Setting the IMS Server location	17
Supported web browsers	17
Supported Thin Clients	18
Authentication	19
Encentuate password	19
USB Key password	20
Active Directory password	20
User-defined secrets	21
System-defined secrets	21
Additional authentication	22
USB Key	22
OTP token	23
Types of OTP tokens	23
Solution overview	24
RFID	26
Active RFID (ARFID)	27
Fingerprint	28
Authorization code	28

Online authorization code	29
Offline authorization code	30
Mobile ActiveCode (MAC)	31
Solution overview	31
Key features and benefits	32
Mobile ActiveCode API	33
Enabling applications with MAC	33
Multiple second factor support	35
Presence Detectors	37
Sonar devices	37
Active RFID	41

Part II: Installation and Setup 44

AccessAgent Setup	45
Installing AccessAgent	45
Setting up the IMS Server location	50
Verifying the program folders and registry entries	50
Program folders	50
Registry entries	51
Changing the AccessAgent banner	51
Setting a transparent screen lock	52
Launching applications from EnGINA	54
Setting automatic sign-on for Java applications	57
Mapping network drives using EnWinNetUse	58
IMS Server Setup	61
Using the IMS Configuration Utility	62
Enterprise directory setup	62
About enterprise directories	63
Setting up a new enterprise directory	64
Setting up an ADSI application connector	66
Setting up an Active Directory (ADSI) Forest	66
Setting up other application connectors	67
Basic configuration keys	68
Advanced configuration keys	68
Preparing the IMS database	70
Prerequisites for Microsoft SQL Server 2000	70
Prerequisites for Microsoft SQL Server 2005	71
Prerequisites for Oracle	71
Improving IMS Server performance	72
Optimizing memory for the IMS Server	75
Increasing the number of concurrent users	76
Increasing the database connection pool size	77
Increasing the maximum number of RADIUS packets	78
Enhancing server scalability and availability	78
Managing IMS clusters	79
IMS load balancing architecture	80
About the Microsoft Network Load Balancer (NLB)	81
Setting up IMS clusters using Microsoft NLB	81

Checklists and assumptions	82
Setting up clusters for new deployments	82
Setting up clusters for existing deployments	83
Creating IMS clusters	84
Maintaining IMS clusters	91
Disassembling IMS clusters	91
Upgrading each IMS Server	92
Adding the IMS Server back to the cluster	92
Copying an upgrade to the other hosts	93
Reassembling the cluster	93
Using AccessAdmin	93
Role assignment features	95
Reassigning roles for Helpdesk users	95
Automatic role assignment for large deployments	96
Managing remote access for IMS Servers	97
Setting up IMS proxies on dedicated servers	98
Setting up IMS proxies on existing web applications	99
Port forwarding	99
Placing IMS in DMZ	100

Provisioning Setup 101

Provisioning API	101
About Encentuate Provisioning Agent	102
Solution overview	103
Deployment options	103
General prerequisites	104
Workflow and use case	104
Installation and configuration	105
Installing the Encentuate provisioning agent	105
Configuring the Encentuate Provisioning Agent	106
Starting the Encentuate provisioning agent	115
Configuring Encentuate provisioning agent (Advanced)	115
ADAM configuration	116
Policy settings	116
Issues and notes	116

Strong Authentication Setup 119

Encentuate password setup	119
ActiveDirectory password setup	120
Recommended settings	120
Additional information	120
USB Key setup	121
OTP Token setup	123
Deployment options	123
Workflow and use cases	123
Uploading OTP Token data files to IMS Server	124
Registering users	125
Assigning or revoking OTP Tokens	126
Searching for OTP Tokens by serial numbers	126
Authenticating users with OTP Tokens	127
Resetting time-based OTP Tokens	128
Resetting OATH-based OTP Tokens	129

Installing OTP token support	130
Installing VASCO OTP library files	130
Configuring RADIUS authentication for applications	130
Enabling user registration through AccessAdmin	130
Setting ActiveCode-enabled authentication service bindings	131
Policy settings	132
Advanced settings for OATH-based OTP	133
Issues and notes	133
Mobile ActiveCode setup	134
RFID setup	135
Active RFID setup	136
Fingerprint setup	139
Multiple second factor support setup	141
AccessAssistant and Web Workplace Setup	143
Installing AccessAssistant and Web Workplace	144
Deploying AccessAssistant or Web Workplace.	145
AccessAssistant and Web Workplace settings	147
Upgrading AccessAssistant and Web Workplace	147
Embedding Web Workplace in the enterprise portal	148
Managing policies	148
Setting automatic Web sign-on for AccessProfiles	149
Maintaining existing AccessProfiles	150
Creating Web AccessProfiles	154
Synchronizing system data with the IMS Server	157

Part III:Monitoring and Management 160

Microsoft Operations Manager (MOM)	161
About MOM	161
Importing the MOM Management Pack for the IMS Server	165
MOM prerequisites	165
IMS Server prerequisites	166
Installing the MOM agent on the IMS Server	166
Setting up IMS Server logging for Syslog	167
SNMP and JMX Support	169
About SNMP	170
About JMX	170
SNMP and JMX system requirements	171
SNMP support	171
JMX support	171
Monitor IMS Server, Tomcat, and JVM	171
Information to be monitored	172
IMS Server notifications	174
Installing AdventNet JMX-SNMP Adaptor on the IMS Server	174
Setting up IMS Server for SNMP and JMX support	174
Testing SNMP and JMX	175
Using the JMX HTTP Adaptor	175
Using the AdventNet MibBrowser tool	176
Testing the MC4J software	176

Auditing and Reporting	177
Viewing the event log	177
Generating database views	178
Tracking successful/unsuccessful logons and logoffs	178
Creating custom events	181

Part IV: Usage and Recovery Workflows 184

Usage Workflows	185
Managing workflows for personal workstations	185
Setting up Encentuate IAM Enterprise (personal workstation)	185
Signing up from personal workstations	186
Personal workstation workflow	187
Personal workstation logon	188
Personal workstation lock	188
Personal workstation unlock	189
Personal workstation logoff	189
Managing workflows for shared workstations	189
Setting workflows for shared desktops	191
Setting up Encentuate IAM Enterprise (shared desktop)	191
Signing up for shared desktops	192
Shared desktop workflow	193
Setting workflows for private desktops	195
Setting up Encentuate IAM Enterprise (private desktops)	196
Signing up for private desktops	198
Private desktop workflow	199
Setting workflows for roaming desktops	203
Prerequisites for roaming desktops	204
Terminal Server workflow for roaming desktops	204
Citrix	212
Recovery Workflows	217
Recovery workflows for user issues	217
Forgetting the Encentuate password (online)	217
Forgetting the Encentuate password (offline)	218
Forgetting the USB Key password (online)	219
Forgetting the USB Key password (offline)	220
Forgetting or losing the USB Key (online)	222
Forgetting or losing the USB Key (offline)	224
Forgetting or losing the RFID card (online)	225
Forgetting or losing the RFID card (offline)	227
Recovery workflows for computer issues	228
Cannot unlock the computer successfully (shared workstation)	228
AccessAgent is not installed	228
Recovery workflows for server issues	229
IMS Server is unavailable	229
The IMS Server has crashed	230
The database server has crashed	230
IMS keystore recovery	231
Recovering the CA keystore	231
Recovering the SSL keystore	233
Recovering the log signing keystore	233

Recovering the startup password	233
---------------------------------------	-----

Part V:Advanced Configuration 236

AccessAgent for Citrix 237

About Citrix MetaFrame	237
Installing AccessAgent on a Citrix client	238
Installing AccessAgent on a MetaFrame server	238
Logging in to MetaFrame without local AccessAgent installed	239
Using the Active Directory password as the Encentuate password	240
Do not use Active Directory password as Encentuate password	240
Caching logon credentials on Citrix Server	241
Using a custom IMS Bridge (not recommended)	241
Logging in to MetaFrame with local AccessAgent installed	243
Synchronizing Wallet contents	244
Local AccessAgent and IMS Server synchronization	244
Remote AccessAgent and IMS Server synchronization	245
Policy settings for remote AccessAgent	245

Roaming Sessions 247

About roaming sessions	247
System requirements	248
Installing roaming sessions	248
Installing roaming sessions on Terminal Server	249
Installing AccessAgent (Terminal Server)	249
Terminal Services configuration	249
Enabling auto-fill of Windows credentials in RDP Client	250
Terminal Server policy settings	251
Installing roaming sessions on Citrix	253
Installing AccessAgent (Citrix)	253
MetaFrame Presentation Server settings	254
Terminal Services configuration	255
Enabling auto-fill of logon credentials in ICA Client	255
Citrix policy settings	256

Thin Client 259

About Thin Clients	259
Enabling port redirection and mapping	260
ICA client connecting to a Citrix Server	260
RDP client connecting to a TS/Citrix Server	262
Setting the server's AccessAgent policies	264
Starting up the Thin Client	264
Managing roaming sessions with RFID	265
Monitoring authentication devices on remote client machines	266
Additional Thin Client tips	266

Appendices 270

Deployment Tips 271

Switching to another IMS Server	272
Copying AccessProfiles between IMS Servers	272

Deleting a user without revoking	273
Promoting a user to Administrator	273
Enabling/Disabling autoplay for removable drives	274
Improving AccessAgent performance	274
Specifying the IMS DB user account	274
Configuring the ADAM Server	274
Turning off authentication for AccessAdmin	278
Configuring the IMS Server download port	279
Enabling RFID readers for AccessAgent running in VMware	280
Modifying AccessAdmin web pages	280
Uninstalling AccessAgent in private desktops	281
Private desktop with Websense internet content filtering services	281
Troubleshooting	283
Definitions of policies	299
Setting policy priorities	299
Legend	301
Policies	303
Encentuate IMS Bridge for Citrix	375
Creating a rule in MOM	377
Testing Redirection of COM Port	383
Prerequisites	383
Running the check	383
Mapping MOM Log Parameters to IMDS Server Log At-tributes	387
IMSLOGSystemOps	387
IMSLOGUserActivity	388
IMSLOGUserService	388
IMSLOGUserAdminActivity	389
IMSLOGSystemMgmtActivity	390
Device Monitoring-Related Registry Entries	391
Shared Workstation & Monitoring-Related Registry Entries	393
VBScript for Registering and Starting ObsService	395
Configuring Auto-Logon to Servers	397
Configuring auto-logon for RDP clients	397
Configuring auto-logon for ICA clients	398
Configuring MAC Settings at IMS Server	399

Configuring a message connector	403
Enabling MAC for Applications and Users	407
Provisioning a user for MAC	407
Enabling MAC	407
Enabling MAC for SSL VPN	407
Enabling MAC for a user	410
Configuring the RADIUS Interface at IMS Server	413
Enabling RADIUS	413
Adding a new RADIUS client configuration	415
Integrating with Aventail SSL VPN	417
Configuring the VPN Server	417
Configuring authentication servers	418
Configuring realms	418
Configuring services	418
Configuring resources	419
Configuring Aventail WorkPlace	419
Configuring Access Control	420
Configuring SSL settings	420
Completing the configuration	421
Integrating with Juniper SSL VPN	423
System requirements	423
Supported software versions	423
Supported Web browsers	424
Supported second factors	424
Network requirements	425
Configuring authentication servers	425
Configuring user realms	426
Configuring signing-in	426
Configuring Web resources profiles	427
Configuring terminal services resources	428
Configuring SSL settings	429
Embedding application links	429
Enterprise portal	429
Web application	429
Windows Terminal Server or Citrix server	430
Web Workplace portal page	430
Integrating with F5 SSL VPN	431
System requirements	431
Supported software versions	431
Supported Web browsers	432
Supported second factors	432
Network requirements	433
Configuring user group	433
Customize WebDAV	434
Configuring Web application resources	436
Configuring terminal server resources	437

Embedding application links in an enterprise portal	437
Web application	437
Windows Terminal Server or Citrix server	438
Web Workplace portal page	438

Integrating an Application with MAC Using SOAP API 439

Basic concepts	439
Required components	440
Logging on with an MAC	440
Using API	442
API Data	442
resultCode	442
resultString	444
ResultMessage	444
API operations	445
requestOtp	445
requestOtpWithPasscode	447
verifyOtp	449
Enabling MAC authentication for an application using the SOAP API	450
Deployment scenarios	451
Developing the SOAP client	452
IMS Server configuration	453
WDSL	454

Glossary and Abbreviations 457

About This Guide

Welcome to the Encentuate IAM Enterprise Deployment Guide.

Use this deployment guide to deploy, configure, and troubleshoot the different components of Encentuate IAM Enterprise.

Purpose

This guide provides procedures to help deploy, install, and test Encentuate IAM Enterprise. It aims to cover the functionality and setup options of the product without focusing internal implementation details (i.e., describes what the product does and how to set it up).

Audience

The target users for this deployment guide are highly technical users that can understand how an Encentuate product can be enhanced and customized for a specific customer's use.

What's in this guide

[Part I: Introduction to Encentuate IAM Enterprise](#) provides an overview of Encentuate IAM Enterprise and common authentication methods.

[Part II: Installation and Setup](#) contains instructions for successfully installing and configuring the main components of Encentuate IAM Enterprise, such as IMS Server, Provisioning API, Access Agent, AccessAssistant and Web Workplace, and suggested methods for achieving strong authentication.

[Part III: Monitoring and Management](#) contains chapters on the Microsoft Operations Manager (MOM), SNMP and JMX, and tools for auditing activities and events in Encentuate IAM Enterprise.

[Part IV: Usage and Recovery Workflows](#) provides information on managing workflows for supported desktop configurations (e.g., personal, shared, private, and roaming) and suggested recovery workflows for any issues encountered with Encentuate IAM Enterprise.

[Part V: Advanced Configuration](#) comprises useful information on setting up AccessAgent for Citrix, roaming sessions on Encentuate IAM Enterprise, and for a Thin Client configuration.

[Appendices](#) provides additional information on troubleshooting, deployment tips, and other ways of customizing and enhancing Encentuate IAM Enterprise according to the organization's needs.

[Glossary and Abbreviations](#) defines all the commonly-used terms and abbreviations used throughout the guide.

Document conventions

Refer to this section to understand the distinctions of formatted content in this guide.

Main interface elements

The following are highlighted in bold text in the guide: dialog boxes, tabs, panels, fields, check boxes, radio buttons, fields, buttons, folder names, policy IDs/names, and keys. Examples are: **OK**, **Options** tab, and **Account Name** field.

Navigation

All content that helps users navigate around an interface is italicized (e.g., *Start >> Run >> All Programs*)

Cross-references

Cross-references refer you to other topics in the guide that may provide additional information or reference. Cross-references are highlighted in green and display the referring topic's name (e.g., [Document conventions](#)).

Hyperlinks

Hyperlinks refer you to external documents or web pages that may provide additional information or reference. Hyperlinks are highlighted in blue and display the actual location of the external document or web page (e.g., <http://www.encentuate.com>).

Scripts, commands, and code

Scripts, commands, or code are those entered within the system itself for configuration or setup purposes, and are usually formatted in a Courier font.

for example,

```
<script language="JavaScript">  
  
<!--  
  
    ht_basename = "index.php";  
  
    ht_dirbase = "";  
  
    ht_dirpath = "/" + ht_dirbase;  
  
//-->  
  
</script>
```

Tips or Hints



Tips or hints help explain useful information that would help perform certain tasks better.

Warnings



Warnings highlight critical information that would affect the main functionalities of the system or any data-related issues.

PART I: INTRODUCTION TO ENCENTUATE IAM ENTERPRISE

Part I: Introduction to Encentuate IAM Enterprise

Use this part of the guide to learn more about Encentuate IAM Enterprise and other related concepts. Refer to the following chapters:

- [About Encentuate IAM Enterprise](#), which provides an overview of the Encentuate IAM Enterprise system, the main product components, and minimum system requirements.
- [Authentication](#), which discusses the common authentication methods used with Encentuate IAM Enterprise, additional tools that facilitate stronger authentication, and managing multiple second factor support.
- [Presence Detectors](#), which describes the currently supported presence detectors, which range from sonar devices to Active RFIDs.

About Encentuate IAM Enterprise

The Encentuate® Identity and Access Management (IAM) empowers enterprises to automate access to corporate information, strengthen security and enforce compliance at the enterprise end-points. With Encentuate, enterprises can efficiently manage business risk, achieve regulatory compliance, decrease IT costs, and increase user efficiency.

This chapter covers the following topics:

- [Encentuate IAM Enterprise features](#)
- [System overview](#)
- [Minimum system requirements](#)

Encentuate IAM Enterprise features

Encentuate IAM Enterprise delivers the following capabilities, without requiring changes to the existing IT infrastructure:

Enterprise single sign-on with workflow automation

With Encentuate Single Sign-On (ESSO), users can enjoy fast access to all corporate applications (e.g., web, desktop, TTY and legacy) and network resources with the use of a single, strong password on personal and shared workstations.

This feature helps enterprises increase employee productivity, lower IT Helpdesk costs, and improve security levels by eliminating passwords and the effort of managing complex password policies.

Encentuate IAM Enterprise improves speed-to-information by up to 85% via SSO and workflow automation on shared and personal workstations. Users can automate the entire access workflow (e.g., application login, drive mapping, application launch, single sign-on, navigation to preferred screens, multi-step logins, etc.).

Single Sign-Off and configurable desktop protection policies ensure protection of confidential corporate applications from unauthorized access. If a user walks away from a workstation without logging out, Encentuate IAM Enterprise can be configured to enforce inactivity timeout policies (e.g., configurable screen locks, application logout policies, graceful logoff, etc.).

Strong authentication for all user groups

Encentuate IAM Enterprise provides strong authentication for all user groups – inside and outside the corporate perimeter – to prevent unauthorized access to confidential corporate information and IT networks. The solution leverages multi-factor authentication devices, such as USB smart card tokens, building access badges, proximity cards, mobile devices, photo badges, biometrics, and one-time password (OTP) tokens.

In addition to comprehensive support for authentication devices, Encentuate IAM Enterprise focuses on leveraging existing identification devices and technologies for authentication. Encentuate IAM Enterprise also provides iTag, a patent-pending technology that can convert any photo badge or personal object into a proximity device, which can be used for strong authentication.

Comprehensive session management capability

As organizations deploying more shared workstations and kiosks, more users can roam and access information from anywhere without having to return to their personal PCs. Shared and roaming scenarios pose severe security threats. When users walk away without logging off from workstations or share generic logins, they risk exposing confidential information to unauthorized access. Any attempt to tighten security, enforce unique user logins, and comply with regulations leads to users being locked out of workstations, which results in efficiency losses.

With Encentuate IAM Enterprise, organizations can increase user convenience and improve information security through session management or fast user switching capabilities, depending on the access needs user groups. Users can quickly sign-on and sign-off to shared workstations without using the Windows domain login process, picking up their work where they left off.

Additionally, fast user switching on private desktops allows users to maintain multiple unique user desktops on the same workstation, preserving each user's applications, documents, and network drive mappings.

If a user walks away from a session without logging out, Encentuate IAM Enterprise can be configured to enforce inactivity timeout policies. Encentuate IAM Enterprise also supports hybrid desktops where organizations combine different session management capabilities to meet the needs of their user community.

User-centric access tracking for audit and compliance reporting

With Encentuate IAM Enterprise's Audit & Compliance functionality, organizations can consolidate data, manage user-centric, secure, and tamper-evident audit capabilities across all end-points (e.g., personal or shared workstations, Citrix, Windows Terminal Services, or browsers).

When combined with Encentuate's strong authentication capabilities, the user-centric audit logs ensure secure access to confidential corporate information and accountability at all times. The logs provide the meta-information that can guide compliance and IT Administrators to a more detailed analysis – by user, by application, or by end-point.

In addition, this information is collated in a central relational database facilitating real-time monitoring and separate reporting with third party reporting tools.

Organizations can also leverage the end-point automation framework to audit custom access events for any application – without modifying the application or leveraging the native audit functionalities.

Secure remote access for easy, secure access anywhere, anytime

Encentuate Secure Remote Access provides browser-based single sign-on to all applications (e.g., legacy, desktop, and Web) from outside the firewall. Organizations can effectively and quickly enable secure remote access for their mobile workforce without installing any desktop software and modifying application servers.

Remote workers require only one password, and an optional second authentication factor, to access corporate information from remote offices, home PCs, and PDAs. Once access is granted, users can single sign-on to corporate applications by clicking on the application links available in the Encentuate portal. Access can be further protected through an SSL VPN.

Integration with user provisioning technologies

Encentuate IAM Enterprise combines with best-of-breed user provisioning technologies to provide end-to-end identity lifecycle management. New employees, partners, or contractors get fast and easy access to corporate information upon being provisioned. Once provisioned, users can leverage single sign-on to access all their applications on shared and personal workstations with one password.

Users are never required to register their user names and passwords individually as their credentials are automatically provisioned.

System overview

Encentuate product components

The following are the main components of Encentuate IAM Enterprise. A typical installation will involve some of the components. For more information, contact your Administrator.

Component	Description
AccessAgent	Client software that manages the user's identity, enabling sign-on/sign-off automation, session management, and authentication management.
Encentuate AccessAdmin	Management console used by individuals with the Administrator Role and/or the Helpdesk Role to administer IMS Server, and to manage users and policies.
Encentuate AccessAssistant	Web-based interface used to provide password self-help. Users use AccessAssistant to get the latest credentials to log on to their applications. The Web automatic sign-on feature enables users to log on to enterprise Web applications by clicking on links, without the need to remember the passwords for individual applications.
AccessStudio	Interface used to create AccessProfiles required to support sign-on/sign-off automation and fortified passwords.
Encentuate IMS Bridge	IMS Service Modules that enable applications to use IMS Server as an authentication server.
Encentuate IMS Connector	Add-ons to IMS Server that enable IMS Server to interface with other applications as a client, extending the capability of IMS Server.
IMS Server	Integrated management system that provides a central point of secure access administration for an enterprise. It enables centralized management of user identities, AccessProfiles, and authentication policies. It also provides loss management, certificate management, and audit management for the enterprise.
Encentuate IMS Service Module	Add-on modules that extend the basic services (user management, policy management, and certificate issuance, etc.) provided by IMS Server.
Encentuate Signature HSM	Hardware security module that generates, stores, and secures cryptographic signing keys. It provides a highly secure hardware environment for safe keeping of signing keys that are used to issue certificates.

Component	Description
Encentuate USB Key	Encentuate's customized token that combines the utility and capacity of Flash RAM, the security of a smart card, and the universal connectivity of Universal Serial Bus (USB) into one package. Encentuate's USB Key is a portable and personalized device for storing user names, passwords, certificates, encryption keys, and other security credentials.
Encentuate USB Key Utility	Add-on module to AccessAgent that provides Administrator with functions to reset Encentuate USB Keys.
Encentuate USB Proximity Key	Encentuate USB Key augmented with an RFID capability. Hence, an USB Proximity Key combines the functions of an Encentuate USB Key with a RFID card.
Encentuate Web Workplace	Web-based interface that gives users the ability to log on to enterprise Web applications by simply clicking on links, without the need to remember the passwords for individual applications. It can be integrated with customer's existing portal or SSL VPN.

User roles

The following table lists the roles of users who directly interact with Encentuate IAM Enterprise:

User Class / Role	Description	Examples
Administrator	Manages users, policies, and IMS Server.	<ul style="list-style-type: none"> • System Administrator in IT department • Central organization-wide Administrator
Helpdesk	Manages user groups, resets password, issues authorization codes, and revokes users access rights.	<ul style="list-style-type: none"> • IT Helpdesk personnel • Department Administrator
User	Uses AccessAgent and AccessAssistant for sign-on automation and access to application credentials.	<ul style="list-style-type: none"> • Executives • Engineers • Accountants • Doctors • Nurses • Home PC user

Policies

Encentuate IAM Enterprise uses policies to control the behavior of its components. These policies are configurable, thus allowing the product to meet the requirements of specific customers. Policies have different visibilities and scopes, and are managed by different roles.

Each policy is identified by its policy ID that is prefixed with "pid", for example, **pid_wallet_authentication_option**.

Policies are applicable system-wide, or only to certain groups of users. The applicability of a policy is determined by its scope, which can be System, User, or Machine.

- **System:** Policy is system-wide
- **User:** Policy affects only a specific user
- **Machine:** Policy affects only a specific machine

System and User policies are configured with AccessAdmin. Changes to these policies are propagated to clients the next time AccessAgent synchronizes with IMS Server.

Machine policies are implemented as Windows registry entries on individual machines, and are configured using AccessAdmin. Through AccessAdmin, System and machine policies can be modified by the Administrator, but can only be viewed by the Helpdesk user. However, User policies can be modified by both the Administrator and Helpdesk user.

A policy may be defined for different scopes. For example, **pid_desktop_inactivity_mins** may define the desktop inactivity timeout duration for a machine or for the entire system.

If this policy is defined for both scopes, set a priority in case the time-out value is different for the machine and for the entire system. For more information on setting policy priorities, see [Setting policy priorities](#).

Policies may be dependent on other policies. For example, **pid_enc_hot_key_action** is only effective if **pid_enc_hot_key_enabled** is set to **True**. If the latter is set to **False**, any setting for **pid_enc_hot_key_action** will not have any effect on users.

Some groups of policies have overlapping scopes. For example, all these policies have system scopes but the range of entities that they affect are different:

- **pid_wallet_inject_pwd_entry_option_default** (defines the default password entry option for all authentication services and applications)
- **pid_auth_inject_pwd_entry_option_default** (defines the default password entry option for a specific authentication service)

- **pid_app_inject_pwd_entry_option_default** (defines the default password entry option for a specific application)

In general, application-specific policies override authentication service-specific policies, which in turn, override general Wallet policies. In this case, when the other two policies are not defined for a particular authentication service or application, **pid_wallet_inject_pwd_entry_option_default** is used.

However, if **pid_auth_inject_pwd_entry_option_default** is defined for an authentication service, it will override **pid_wallet_inject_pwd_entry_option_default** when a default password entry option is needed for the authentication service. Similarly, if **pid_app_inject_pwd_entry_option_default** is defined for a particular application, it will override the other two policies.

In a similar way, user-specific policies override system-wide policies. Hence, if a policy has both user and system scopes, for example, **pid_auth_accounts_max**, the user scope setting is always effective if it is defined. If the user scope setting is not defined for a particular user, the system scope setting will become effective.

A Command Line Tool (CLT) allows Administrators to view and set policy priorities. For more information, see [Setting policy priorities](#).

To set a policy, determine its scope and its dependencies on other policies. The complete list of policies can be found in [Definitions of policies](#). Some policies have a Notes section that indicate their dependencies on and relationships with other policies. Read the notes carefully.

To set a policy:

- ① Look for the policy in [Definitions of policies](#).
- ② Review the notes and determine if there are any dependencies on other policies or configuration settings. If there are dependencies, ensure that the other policies and configuration settings are set appropriately.
- ③ Identify the available scopes (in the **Scope** column) of the policy. If there are multiple scopes, choose a scope and set the corresponding policy priority. For more information, see [Setting policy priorities](#).
- ④ (System scope) Log on to AccessAgent as Administrator, launch AccessAdmin, navigate to System Policies (or Authentication Service Policies/Application Policies, if it is applied to a particular authentication service or application), and look for the setting that matches the policy's **IMS Entry** column.
- ⑤ (User scope) To modify the policy for a particular user, log on to AccessAgent as Administrator or Helpdesk, launch AccessAdmin, search for the user, and look for the setting that matches the policy's **IMS Entry** column.
- ⑥ (User scope) To modify the policy in a policy template, log on to AccessAgent as Administrator, launch AccessAdmin, navigate to the desired policy template, and look for the setting that matches the policy's **IMS Entry** column.

- 7 (Machine scope) To modify the policy for a particular machine, launch AccessAdmin, navigate to Machine Policies if it is applied to a particular authentication service or application), and look for the setting that matches the policy's **Registry** column, and set it to one of the values indicated in the policy's **Values** column.
- 8 (Machine scope) To set the policy when you install AccessAgent at the target machines, modify them using AccessAdmin.
- 9 The new policy value may only become applicable immediately, after the next synchronization between AccessAgent and IMS Server, or after the machine is restarted. Check the **refreshed on** specification in the policy's **Values** column.

Using Wallets

Wallet is an identity wallet that stores a collection of access credentials and related information (including user names, passwords, certificates, encryption keys, etc.). Each user persona has a Wallet that acts as his personal meta-directory.

A set of authentication factors protects each Wallet. The combinations of authentication factors that can be used to log on to a Wallet are determined by the Wallet's authentication policy (**pid_wallet_authentication_option**). For example, if a user's authentication policy is "USB Key" and "Password + RFID", the user may access his Wallet by using his USB Key with password (password is implicitly required for USB Keys), or his RFID card with Encentuate password.

The layout of a Wallet is flexible so that some parts of the Wallet can be stored only on a specific authentication factor, for example, a private key on a smart card. The Wallet roams to any point of access where AccessAgent is installed. It is similar to Microsoft's Passport, in that it provides a container where users' profile and identity information is aggregated.

However, unlike Microsoft's Passport, the Wallet is under complete user control and management and interfaces with other applications through AccessAgent. The Wallet can be accessed as long as the appropriate combination of authentication factors are presented.

A Wallet that is stored on IMS Server can only be accessed when AccessAgent is online and IMS Server is reachable. To support offline access, Wallets can be cached in the hard disk or in an authentication factor (e.g., USB Key). Wallets can also be in-memory, which can only be used during a particular AccessAgent session.

Whether a Wallet is cached whenever it is accessed is determined by the Wallet caching policy (**pid_wallet_caching_option**).



Certificates and OTP seeds are only created for cached Wallets, stored in either the hard disk or USB Key. In-memory Wallets do not have certificates and OTP seeds.

When a Wallet is cached, a set of locks is created based on the Wallet's authentication policy (**pid_wallet_authentication_option**) and the authentication factors supported by the machine (**pid_second_factors_supported_list**). Each lock protects the Wallet. A lock can be as simple as a password or some other authentication factor, or a combination thereof.

Enable cached Wallet security (**pid_wallet_cache_security_enabled**) to assign user and machine Wallets to the machine it was created. This prevents cached Wallets from being copied and used in other machines. However, this policy should be disabled if cached Wallets are shared among several machines.

The user can access the cached Wallet as long as the user presents a set of authentication factors that can open any of the locks. The set of locks for each Wallet is refreshed with the latest Wallet authentication policy every time the user logs on to the Wallet while IMS Server is available.

Temporary locks may be created in certain scenarios (e.g., offline password reset). Such a lock is removed when the authorization code that is used to create it expires.

Wallets can be revoked by the Administrator or Helpdesk through AccessAdmin. However, revocation of cached Wallets will only be effective the next time the AccessAgent comes online and IMS Server is available.

Minimum system requirements

The requirements listed in this section refer to a typical installation of Encentuate IAM Enterprise.

Supported servers

Hardware requirements (not including database)

- PC with at least 1.2GHz processor clock speed; using Intel Pentium/Celeron, AMD K6/Athlon/Duron, or compatible processor.
- Minimum 256MB of RAM; at least 1GB of RAM recommended (main testing platforms use 1GB RAM).
- At least 300MB free hard disk space.

Network requirements

- Network bandwidth of at least 10Mbps.
- http:// (TCP port 80) and https:// (TCP port 443) traffic to be allowed from AccessAgent clients.
- RADIUS traffic to be allowed from RADIUS clients, if RADIUS authentication is used (to support OTP ActiveCode or Mobile ActiveCode).
- Other network traffic that may be required by IMS Bridges and Connectors (e.g., LDAP, ADSI, messaging gateways).

IMS Server software requirements

- Microsoft Windows 2000 Service Pack 3, Microsoft Windows XP Service Pack 2, or Microsoft Windows Server 2003
- Database software requirements:
 - Microsoft SQL Server 2000
 - Microsoft SQL Server 2000 Desktop Engine (MSDE)
 - Microsoft SQL Server 2005
 - Microsoft SQL Express
 - Oracle Database 9i
 - Oracle Database 10g

Roaming support matrix

Use the roaming support matrix to determine which authentication second factor(s) can be used based on the installed systems for the client machine and remote server.

The following table lists the roles supported combinations of clients, servers, and authentication factors:

Client Machine	Remote Server	Authentication second Factors
Windows 2000 or Windows XP, with local AccessAgent	Terminal Server on Windows 2003	All second factors already supported by AccessAgent
Windows 2000 or Windows XP, with local AccessAgent	Citrix MetaFrame Presentation Server 3.0 on Windows 2003	All second factors already supported by AccessAgent

Client Machine	Remote Server	Authentication second Factors
Windows 2000 or Windows XP, without local AccessAgent	Terminal Server on Windows 2003	Authorization code
Windows 2000 or Windows XP, without local AccessAgent	Citrix MetaFrame Presentation Server 3.0 on Windows 2003	Authorization code
Windows CE (Thin Client), without local AccessAgent	Terminal Server on Windows 2003	RF IDEas pcProx 232 reader (for 125 kHz cards)
Windows CE (Thin Client), without local AccessAgent	Citrix MetaFrame Presentation Server 3.0 on Windows 2003	RF IDEas pcProx 232 reader (for 125 kHz cards)

Setting the IMS Server location

The IMS Server location should normally be set during setup time by setting the `ImsServerName` key in **SetupHlp.ini** appropriately. The AccessAgent installer will automatically download the IMS Server certificate from IMS Server.

If the downloading of the certificate fails during installation, the user will be prompted, but can choose to proceed with the installation.

However, the user cannot sign up or log on unless the certificate is eventually downloaded. This can be done by running *Start >> All Programs >> Encentuate AccessAgent >> Set IMS Server Location*. Alternatively, the same utility can be run by executing **C:\Program Files\Encentuate\SetupCertDlg.exe**.



The Set IMS Server Location utility currently does not allow user to modify the IMS Server name and port number. These will need to be modified by setting the registry entries that correspond to the appropriate machine policies: `pid_ims_server_name` and `pid_ims_download_service_port`.

Refer to the requirements based on the selected client setup (e.g., web-based or Thin Client).

Supported web browsers

For AccessAssistant and Web Workplace, the following Web browsers, in their default settings, are currently tested and supported:

- Internet Explorer 5.0 and above on Windows
- Firefox 1.0 and above on Windows and Linux

Since the product was not specifically designed for the above Web browsers, it is also possible to use other Web browsers. Customers or users should test any other Web browsers with AccessAssistant or Web Workplace before using them.

For AccessAgent, the only supported web browser is Internet Explorer 5.0 and above on Windows.

Supported Thin Clients

- Neoware and Wyse Thin Clients
- Microsoft Windows CE: 4.20, also tested with Microsoft Windows XP Embedded
- RDP connections (to Windows 2003 Server and also RDP to Citrix server installed on Windows 2003 Server) as well as ICA connections (to Citrix Metaframe Server on Windows 2000 and Windows 2003 Servers).
- RFIDEas pcProx serial reader: Model BSE-PCPRXH-232 connected to the Thin Client.

Authentication

One of the key features of Encentuate IAM Enterprise is the ability to support a large variety of authentication factors. This makes it easy for customers who are already using some of these authentication factors to deploy Encentuate IAM Enterprise quickly. Encentuate IAM Enterprise can also meet the various usability, convenience, and security requirements of different customers.

This section covers the following topics:

- [Encentuate password](#)
- [USB Key password](#)
- [Active Directory password](#)
- [User-defined secrets](#)
- [System-defined secrets](#)
- [Additional authentication](#)
- [Multiple second factor support](#)

Encentuate password

The Encentuate password is the primary authentication factor for accessing Wallets. This password is always used to log on to a Wallet except for some special situations.

Once logged on using an Encentuate password, the user can automatically sign on to the applications listed on the Wallet. Users will not have to remember all the passwords of the applications.

USB Key password

A USB Key or smart card is usually secured with a PIN on the device itself. This PIN is known as the USB Key password. However, since most users would be confused by multiple passwords, the policy **pid_enc_pwd_is_usb_key_pwd_enabled** enables the synchronization of the Encentuate password with the USB Key password.

If this policy is set to **True**, the Encentuate password will always be the same as the last changed USB Key password. In this mode, the user can only change the password when logged on to the USB Key. This ensures that the Encentuate password and the USB Key password are always synchronized. This mode should be used for normal users who have only one assigned USB Key.

Power users, who may have more than one USB Key, need to understand that the password for each USB Key may be different. The policy **pid_enc_pwd_is_usb_key_pwd_enabled** should be set to **False** for power users as they are expected to know that the Encentuate password and each USB Key password may be different. For these users, the Encentuate password must be used with other authentication factors (e.g., RFID, ARFID).

Active Directory password

Use the Active Directory password synchronization feature in deployments where Active Directory password is used as the primary password for logon to computers and applications. This feature is especially useful for deployment with a mixture of computers with and without AccessAgent installed.

With this feature enabled, the Encentuate password will always synchronize with the Active Directory password, and users can use the same password to log on to all computers, with or without AccessAgent installed.

If the user changes the Active Directory password while logged on to AccessAgent, AccessAgent will recognize the change and modify the Encentuate password accordingly. However, if the Active Directory password is changed while user is not logged on to AccessAgent (e.g., Active Directory password reset by Administrator), AccessAgent will only recognize that the Active Directory password and Encentuate password are different when the user tries to log on.

In that case, AccessAgent will prompt the user for the secret, to reset the user's Encentuate password and synchronize it with the Active Directory password.

The main features of an installation with Active Directory synchronization enables are:

- The Active Directory password is treated as the master password.
- During logon to AccessAgent, AccessAgent checks with Active Directory, whether the Active Directory account or password is valid and active.

- Password complexity rules must be defined in Active Directory and not in Encentuate IAM Enterprise.
- Password aging policies can be applied at both Active Directory and Encentuate IAM Enterprise.
- AccessAgent takes care of the password synchronization. During a password change attempt by the user, AccessAgent changes the password at both Active Directory and IMS Server.
- When the passwords are out-of-sync, AccessAgent handles the re-synchronization by prompting the user for the secret.

User-defined secrets

By default, Encentuate IAM Enterprise prompts users to specify user-defined secrets during sign-up. User-defined secrets must be set up by users to resolve certain issues, such as password resets.

System-defined secrets

The sign-up process can be simplified by making one system-defined secret (**pid_secret_option**). Each user would be assigned a system-defined secret, and will not be asked to specify a secret during sign-up (or first logon, for a provisioned user). The user would not be prompted for secret a when performing certain actions, such as reset password, Active Directory password re-sync, and offline recovery.

However, users should understand the security vulnerabilities (e.g., password can be reset by Administrator) before implementing such a configuration. If both the Active Directory password synchronization and system-defined secret features are enabled, the sign-up process can be eliminated by enabling the **policy pid_automatic_sign_up_enabled**. New users can log on to AccessAgent with their Active Directory password and do not have to sign up with Encentuate IAM Enterprise.



*If the policy for secret option (**pid_secret_option**) is changed from a user-defined secret to a system-defined secret, users will be automatically migrated to system-defined secret when they log on to AccessAgent. After the automated migration, AccessAssistant and Web Workplace will also support the users' system-defined secret.*

However, there is no support for migration from system-defined secret to user-defined secret. A customer cannot to switch back to user-defined secret once the system has been configured to use system-defined secret.



If a deployment has the Active Directory password synchronization feature enabled and a user is provisioned into IMS Server using a third party provisioning system (e.g., ITIM), the provisioning system may choose to use a random initial Entencuate password. However, since the user will perform an Active Directory password re-sync during initial logon, the user's secret must be specified. Thus, the random initial Entencuate password can only be used if the system-defined secret feature is enabled.

Additional authentication

The AccessAgent user interface can support sign up, logon, and lock/unlock using several authentication factors, from simple passwords to proximity cards, smart cards, USB Keys, and biometrics. The authorization code can be treated as a special authentication factor that is issued by IMS Server.

For the distribution and adoption of second factors, users can perform an initial sign up with only one factor (password), and an optional second factor. Administrators can implement a grace period, during which users can register their selected second factor. Registration of second factors after the initial sign up require the authorization code issued by the administrator or Helpdesk via AccessAdmin (depends on `pid_second_factor_registration_option`).



Administrators must manually set the authentication policy through AccessAdmin after the grace period for the second factor is enforced.

Authentication second factors can be revoked by the Administrator or Helpdesk anytime via AccessAdmin.



Revoking second factors only affect cached Wallets if they are logged on and online (AccessAgent can reach IMS Server). Once a cached Wallet is logged on while online, locks that contain the revoked second factor are removed.

USB Key

The authentication policy always allows USB Keys to be used as a second factor (such as, the **USB Key** option in the user's authentication policy cannot be disabled). The USB Key password is required when logging on to the USB Key.

USB Key is the recommended second factor for personal workstations.

The supported USB Keys are:

- Encentuate USB Key 2.5
- Encentuate USB Key 3.0
- DigiSAFE KeyCrypt
- Charismathics Keys

At present, the Axalto Cryptoflex e-gate with token connector is not yet supported.



USB Keys do not work on Windows 2000 machines with USB 2.0 hubs (internal or external).

OTP token

A One-Time Password (OTP) can also be used as a second authentication factor. An OTP is a randomly-generated password, intended only for one (1) specific user for a specific time or purpose. For most systems, the OTP can be sent to an OTP token or another mobile device.

Encentuate IAM Enterprise support for both time-based OTP (VASCO Digipass) and OATH-based OTP (Authenex A-Key) tokens adds to the list of OTP ActiveCode options.

The OTP displayed on the LCD of an OTP token can be used as an authentication factor to log on to AccessAssistant, Web Workplace, or any application configured to use IMS Server as authentication server through RADIUS. Currently, the only supported OTP tokens are VASCO Digipass GO 3 and Authenex A-Key.

Types of OTP tokens

VASCO Digipass

With one push on the Digipass GO 3's button, an OTP is shown on its LCD. As the Digipass GO 3 is a time-based OTP device, the displayed OTP is purely based on time, and the user does not have to enter anything on the device itself. The user then enters this OTP into the application logon prompt. Depending on the application's authentication method, a separate static password may also be required (e.g., Encentuate password).

According to VASCO's marketing materials, user acceptance of security tools is a crucial factor in guaranteeing the success of security solution implementations.

Digipass GO 3 is affordable and user-friendly. Its use is obvious and simple, and with a normal battery lifetime of at least 5 years, it requires virtually no support or training. If required, the GO 3 can be re-assigned to another user in cases where an employee is promoted, or even leaves the company. The GO 3 can carry corporate logos, branding and custom colors to suit customers' businesses.



VASCO Digipass GO 3

The Digipass GO 3 has been designed for portability. It can be:

- Carried on a key chain.
- Attached to an existing proximity card.
- Worn around the neck.
- Carried in a pocket or purse.

Authenex A-Key

With one push on the Authenex A-Key's button, an OTP is shown on its LCD. As the A-Key is an OATH-based OTP device, the displayed OTP is purely based on the button press event, and the user does not have to enter anything on the device itself. The user then enters this OTP into the application logon prompt. Depending on the application's authentication method, a separate static password may also be required (e.g., Encuentate password).

According to Authenex's marketing materials, one of the greatest challenges in accepting a second factor authentication solution is the need for a simple and mobile solution. The A-Key is multi-functional, offers more security solutions beyond OTP, and has a battery life beyond 5 years.



Authenex A-Key

Solution overview

This section specifies the high-level requirements of the integrated product, as well as the various options for applications that use OTP token for authentication. The product supports the OATH HOTP algorithm.

The features are described as in the next sections.

Two-factor authentication with no client software installation

Without installing additional software on client PCs, users can use two-factor authentication to existing enterprise applications. This is already possible with the use of MAC. Integration with OTP tokens offers customers with the choice of using a time-based or OATH-based OTP token. Currently, the following OTP tokens are supported:

- VASCO Digipass GO 3 (time-based OTP)
- Authenex A-Key OATH-only token without USB interface (OATH-based OTP)

Choice of second factors during authentication

An application can be set up to have a choice among multiple second factors to authenticate with the application.

At logon time, user can choose to authenticate using:

- OTP provided by a token.
- MAC, which can be sent to the user via mobile phone or email. The user may need to append a pre-defined secret (e.g., Encentuate password, enterprise account password, or Administrator-assigned secret) to the MAC.
- Authorization code issued by Helpdesk. The user may need to append a pre-defined secret (e.g., Encentuate password, enterprise account password, or user's secret) to the authorization code.

Centralized policies and control

Through AccessAdmin, an Administrator can:

- Assign an OTP token to a user or revoke it from a user.
- Enable or disable authentication using OTP token for an authentication service.
- For a user, specify whether to use OTP token as the default second factor for accessing AccessAssistant and Web Workplace.

Centralized audit logging

Authentication attempts using OTP token are centrally logged in IMS Server. These audit logs, including those reported by AccessAgent, can be viewed by the Administrator or Helpdesk through AccessAdmin.

RFID

Currently, RFID must be used with the Encentuate password, except for the RFID-only logon and RFID-only unlock scenarios. This is specified as "Password + RFID" in the user's authentication policy. AccessAdmin automatically enables "Password + RFID" authentication if "Password" authentication is allowed for the user.

RFID is one of the recommended second factors to be used for shared workstations, as all the shared workstation workflows are supported. RFID can also be used for personal workstations.

There are many different versions of RFID cards, and some may require different readers and configuration, as indicated below. In particular, iTag, which is an Encentuate-branded RFID smart label, is a Mifare card.

The supported cards include:

- HID 125kHz Proximity Card
- HID iCLASS
- Mifare (Ultralight, 1K, 4K)



This class of cards includes iTag.

The Indala 125kHz Proximity Card is currently not supported.

The supported readers include:

- RF IDEas pcProx Readers (for 125kHz cards)
- RF IDEas AIR ID Contactless Smart Card Readers (for iCLASS and Mifare cards)
- GIGA-TMS Proximity Reader MFR135 (PCMCIA reader for Mifare cards)
- Altrus Mifare Desktop Reader Writer A1 (USB reader for Mifare cards)

Currently, only one of these three types of RFID cards is supported per deployment:

- Mifare card with 32-bit CSN
- Mifare card with greater than 32-bit CSN
- other RFID cards



iTag is a Mifare card with greater than 32-bit CSN.

Reader	HID Prox Card	Indala Prox Card	Casi-Rusco Prox Card	Electronic Marin (EM) Prox Card	iCLASS Card	Mifare Card (32-bit CSN)	Mifare Card (> 32-bit CSN)
GIGA-TMS Proximity Reader MFR135 (PCM-CIA reader for Mifare cards)	✗	✗	✗	✗	✗	✓	✓
GIGA-TMS Proximity Reader PCR300MU (USB reader for Mifare cards)	✗	✗	✗	✗	✗	✓	✓
Altrus Mifare Desktop Reader Writer A1MF (USB reader for Mifare cards)	✗	✗	✗	✗	✗	✓	✓
RF IDEas RDR-7172AKU	✗	✗	✗	✗	✗	✓	✓
RF IDEas RDR-7582AKU	✗	✗	✗	✗	✗	✓	✓
RF IDEas RDR-6082AKU	✓	✗	✗	✗	✗	✗	✗
RF IDEas BSE-PCPRXH-U	✓	✗	✗	✗	✗	✗	✗
RF IDEas BSE-PCPRXH-232 (serial port reader)	✓	✗	✗	✗	✗	✗	✗
RF IDEas RDR-6081AK2 (serial port reader)	✓	✗	✗	✗	✗	✗	✗
RF IDEas BSE-RFID1356I-USB-ID	✗	✗	✗	✗	✓	✓	✓
RF IDEas RDR-6E72AKU	✗	✗	✗	✓	✗	✗	✗
RF IDEas BSE-PCPROXM-U	✗	✓	✗	✗	✗	✗	✗
RF IDEas BSE-OPLHU	✓	✗	✗	✗	✗	✗	✗
RF IDEas RDR-6272-AKU	✗	✗	✗	✓	✗	✗	✗
RF IDEas RDR-6072 BKU	✓	✗	✗	✗	✗	✗	✗
GIGA-TEK Proximity Reader PCR310MU	✗	✗	✗	✗	✗	✓	✓

Active RFID (ARFID)

The user-friendly name for ARFID is "active proximity badge". This is the term that appears on the AccessAgent user interface.

Currently, ARFID must be used in conjunction with the Encentuate password, except for the RFID-only unlock scenario. This is specified as "Password + RFID" in the user's authentication policy. AccessAdmin automatically enables "Password + RFID" authentication if "Password" authentication is allowed for the user.

ARFID is one of the recommended second factors to be used for shared workstations as all the shared workstation workflows are supported. ARFID can also be used for personal workstations.

The currently supported card is the Ensure Technologies XyLoc Key XC-2.

The currently supported reader is the Ensure Technologies XyLoc Lock NL-2.

Fingerprint

Currently, only one-factor authentication is supported for fingerprint. This is specified as **Fingerprint** in the user's authentication policy.

Fingerprint is one of the recommended authentication factors to be used for shared workstations as all the shared workstation workflows are supported. Fingerprint can also be used for personal workstations.

A user can log on or unlock a computer by simply tapping a finger on the sensor (without password) if the user's cached Wallet is present in the hard drive. If the cached Wallet is absent, the user needs to supply the user name (also without password), as IMS Server can compare a supplied fingerprint with existing fingerprints in the database one at a time, due to performance reasons.

The supported readers include:

- DigitalPersona U.are.U 4000B Fingerprint Reader
- UPEK TouchStrip Fingerprint Sensor TFRZ3 (built-in reader on Lenovo Think-Pad)
- UPEK TouchStrip USB Reader TCRZ3
- UPEK Eikon USB Fingerprint Reader TCRE3C

Authorization code

The authorization code is a system-generated code that can be used as a special authentication factor in certain user scenarios. There are two types of authorization codes:

- **Online authorization code:** Used when AccessAgent can connect to IMS Server. For password reset, registration of authentication factors, or temporary bypass of authentication factor.
- **Offline authorization code:** Used when AccessAgent cannot connect to IMS Server. A request code will be shown on AccessAgent. For temporary password reset or temporary bypass of authentication factor.

Administrator or Helpdesk can issue authorization codes via AccessAdmin. The self-service authorization code feature, if deployed, allows users to request for and obtain an authorization code using mobile phone (SMS).



Although the last-issued authorization code for a user can be revoked by the Administrator or Helpdesk via AccessAdmin, such revocation only prevents the user to use the same authorization code again. Any temporary locks created by the authorization code will still remain valid until the original validity period of the authorization code has expired.

Online authorization code

Online authorization codes can be used when AccessAgent can connect to IMS Server. They are required in the following user scenarios:

- **Password reset (online):** The user has forgotten Encentuate password and needs to reset it. AccessAgent will ask for authorization code and secret.



As USB Key passwords cannot be reset through this method, the user should not insert the USB Key when performing this operation.

- **Registration of authentication factors:** The user wants to register a new second factor for his Wallet. AccessAgent will ask for authorization code and password. The second factor must not have been registered before.
- **Temporary bypass of authentication factor (online):** The user has lost the second factor and his Wallet authentication policy requires it. AccessAgent will ask user to present the second factor after entering the user name and password. If user clicks the **...but I do not have** link, AccessAgent will ask for authorization code as a temporary replacement for the second factor.

A temporary password-only lock (expires when authorization code expires) will be created for the Wallet on the machine. Subsequently, the user can log on to the Wallet on this machine by supplying the user name and password, until the authorization code expires.

Online authorization code properties:

- Can be used multiple times for multiple purposes until it expires.
- Period of validity is specified by the Administrator or Helpdesk on AccessAdmin as and when the authorization code is issued.



The available choices for validity period can be configured via the IMS Configuration Utility. Minimum is 1 hour. 1 month is defined as the period from the day of issue to the same day of the next month, such as, exact number of days depends on the month of issue, for example, from August 26, 2008, 3pm to September 26, 2008, 3pm.

- Length of the authorization code can be configured via the IMS Configuration Utility. It should have a minimum of 1 character and maximum of 32 characters.
- Character set: **0123456789ABCDEF**. It is case-insensitive and any hyphens entered are ignored.

Offline authorization code

Offline authorization codes can be used when AccessAgent cannot connect to IMS Server. They are required in the following user scenarios:

- **Password reset (offline):** The user has forgotten the Encentuate password and needs to reset it temporarily. AccessAgent will ask for authorization code and secret.



As USB Key passwords cannot be reset through this method, user should not insert the USB Key when performing this operation.

- **Temporary bypass of authentication factor (offline):** The user has lost the second factor and the Wallet authentication policy requires it. AccessAgent will ask the user to present the second factor after entering the user name and password. If the user clicks on **...but I do not have** link, AccessAgent will ask for authorization code as a temporary replacement for the second factor.

In both user scenarios, a temporary password-only lock (expires when authorization code expires) will be created for the Wallet on the machine. Subsequently, the user can log on to the Wallet on this machine by supplying the user name and password, until the authorization code expires.

Offline authorization code properties:

- Can be used only once as it is issued based on the request code that is displayed on the AccessAgent.
- Request codes are 8 characters long and they change every minute.
- Period of validity is specified by the Administrator or Helpdesk on AccessAdmin as and when the authorization code is issued.



The available choices for a validity period can be configured in the IMS Configuration Utility (minimum of 1 day, maximum of 31 days, with granularity of 1 day). One month is the period from the issue date to the same day of the next month, thus the exact number of days depends on the month of issue (e.g., from August 26, 2008, 3pm to September 26, 2008, 3pm).

- Offline authorization codes are 16 characters long.

- Default character set for both the request code and authorization code: **Z3467ACEFHJKRWXY**. It is case-insensitive and any hyphens entered by user are ignored.



Supported character sets can be configured via the IMS Configuration Utility.

Mobile ActiveCode (MAC)

An Encentuate Mobile ActiveCode is a one-time password (OTP) that is randomly generated and event-based. MAC is generated on IMS Server and delivered via a second channel, such as text services (Short Message Service) on mobile phones. It is used for strong authentication.

The use of MAC enhances the security of traditional password-based authentication for applications, because a MAC is a random password that can only be used once by an authorized user. Combined with alternative channels and devices, MAC provides effective second factor authentication.

Solution overview

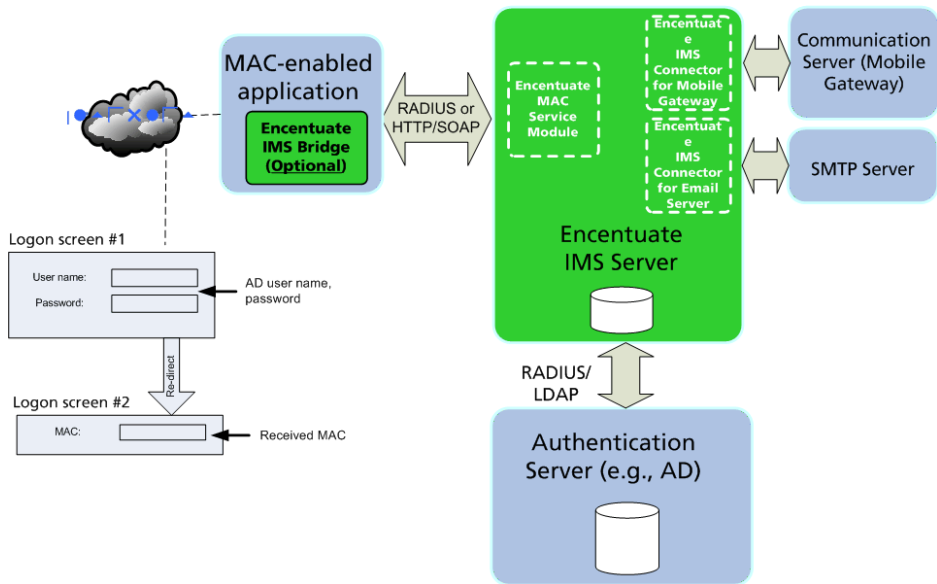
For a typical logon to an application, the user launches the application logon interface. The user then enters the application user name and password. For example, if the application is authenticated against Active Directory, the user enters an Active Directory user name and password.

The authentication request is re-directed to the IMS Server. The IMS Server verifies the logon credentials and delivers an MAC to the user's pre-registered e-mail or mobile phone. The application returns a screen to the user, to enter the MAC.

After receiving the MAC, the user enters the MAC on the application logon interface. Upon submission, the MAC verification request is re-directed to the IMS Server. The user can access the application after successful MAC verification.

If the logon interface is customizable, the user can also choose a preferred channel from the logon interface to send the MAC.

Refer to the following architecture diagram.



:Architecture overview of MAC

Key features and benefits

The Encentuate MAC provides the following benefits:

■ Lower total cost of ownership

- No need to buy additional tokens. You can leverage on what the user already has.
- No need to distribute tokens.
- No license or token renewal fees.

■ Improve user convenience

- No client software required.
- No need to carry an additional token.
- You can leverage on what the user already has for strong authentication to multiple remote services.

■ Strengthen security

- Improves access security through single-use passwords.
- Improves compliance through better audit reporting.

■ Easy to deploy

- Works with any e-mail service or SMS-enabled mobile device.
- Works with any remote access gateways that can be redirected to IMS Server for RADIUS authentication.
- Supports web request for MAC.
- Easy upgrade to the full Encentuate IAM Enterprise solution.

■ Convenient usage

- Multiple channels of delivery: SMS, e-mail, software generation.
- Web-based self-registration for new users.
- Registered users of Encentuate IAM Enterprise are automatically enabled to receive the MAC for remote access.
- Automate sign-on to remote applications through AccessAgent for Windows, AccessAgent for Citrix, and AccessAgent for Terminal Services.

■ Centralized management

- Configurable character set. Administrators may specify the length and the character type to be used for the MAC.
- Centralized management of all users.
- Centralized tracking of all remote application access.

Mobile ActiveCode API

The Encentuate Mobile ActiveCode is a short-term authentication code controlled by Encentuate IAM Enterprise. Mobile ActiveCode enhances the security of traditional password-based authentication for applications, since a Mobile ActiveCode is a random password used once by an authorized user. Combined with alternative channels and devices, Mobile ActiveCode provides effective second factor authentication.

The Encentuate IAM Enterprise SOAP API for Mobile ActiveCode enables third-party applications to integrate with IMS Server using SOAP, to achieve strong authentication with Mobile ActiveCode.

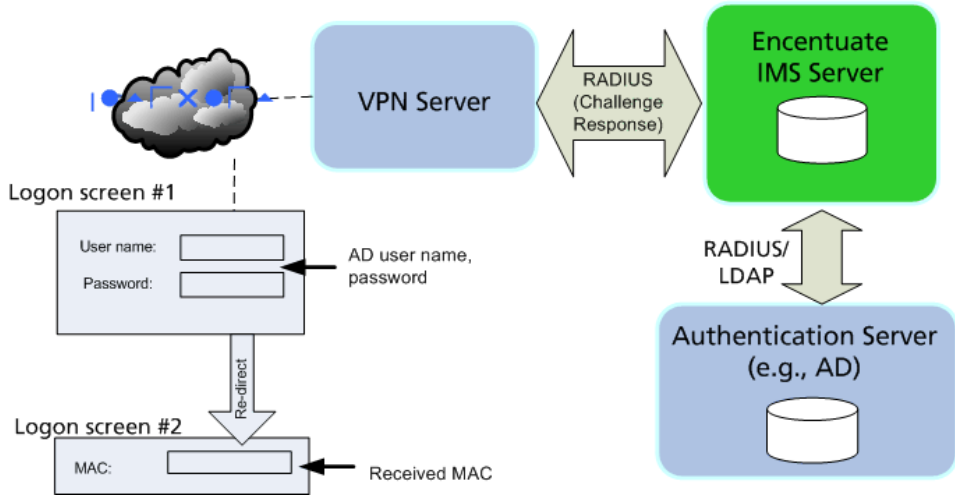
Enabling applications with MAC

The Encentuate MAC can be used to authenticate two types of applications:

- Applications supporting RADIUS such as VPN Servers
- Web applications

Enabling applications supporting RADIUS (VPN servers)

Applications supporting RADIUS must be re-configured to redirect its authentication to the IMS Server, which does the actual verification of the MAC and can allow or disallow users to log on to the application. Refer to the following architecture diagram.

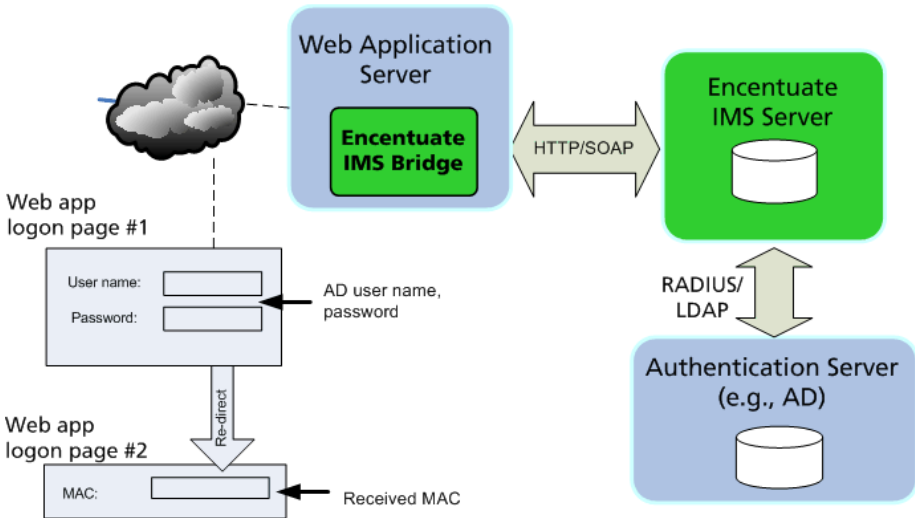


:Architecture overview of MAC for VPN logon

Web applications

These are applications where the application server authentication module can have an additional plug-in, called an Encentuate IMS Bridge. Enabling MAC-based authentication for such applications require an Encentuate IMS Bridge. The IMS Server provides HTTP/SOAP APIs, which can be used by the IMS Bridge to authenticate, request for an MAC and verify the MAC.

Refer to the next architecture diagram.



:Architecture Overview of MAC for Web application logon

Multiple second factor support

AccessAgent can simultaneously support all the authentication second factors mentioned in the sections above within a single deployment. Each user can register multiple second factors (e.g., fingerprint, two USB Keys, and three RFID cards). The combinations of authentication factors that the user can use for logging on are determined by the user policy **pid_wallet_authentication_option**.

However, each workstation can only use one type of second factor, such as, **pid_second_factors_support_list** can only contain one value for each workstation.

Currently, the only exception to this rule is for the following case: **Fingerprint and RFID on one workstation**. This combination is useful for shared workstations that are accessed by users who may or may not have RFID cards issued.

In this setup, a workstation can have both a fingerprint reader and an RFID reader. A user can choose to log on with either fingerprint or RFID card, but not with both (e.g., tap RFID card, and then present fingerprint).

The authentication factors that a user can use for logging on are still determined by his Wallet authentication policy (**pid_wallet_authentication_option**), which may take on any of the following combinations of values:

- Password
- Fingerprint
- Password, or Fingerprint
- RFID+Password
- Password, Fingerprint, or RFID+Password

The supported devices include:

- All the supported RFID cards and readers listed in [RFID](#) section.
- All the supported fingerprint readers listed in [Fingerprint](#) section.

Presence Detectors

A presence detector is a device that can detect the presence of a user in its vicinity. When affixed to a computer, it can notify an application (AccessAgent, in this case) when a user is in front of the computer or goes away. This can enhance the user experience as users do not need to manually lock the computer when leaving the computer for a brief moment.

It is good practice to set the desktop inactivity policy (`pid_desktop_inactivity_action`) so that AccessAgent locks the computer after a specified period of inactivity. However, if the desktop inactivity time-out (`pid_desktop_inactivity_mins`) is configured to be too long, another user may use the previous user's AccessAgent session. On the other hand, making the inactivity period too short also becomes inconvenient to the original user as the desktop may lock frequently.

This chapter covers the following topics:

- [Sonar devices](#)
- [Active RFID](#)

Sonar devices

The RF IDEas sonar-based presence detector (pcProx-Sonar) is another variation in the proximity technologies. This is not a badge or card reader, but a presence detector. This can be used to lock a workstation immediately when the user walks away without waiting for the desktop inactivity time-out. The behavior can be configured to be very similar to ARFID.

However, the difference between ARFID and pcProx-Sonar is that an ARFID badge has a unique ID which can be used to identify a user but pcProx-Sonar cannot be used to identify a user as it does not have any ID.

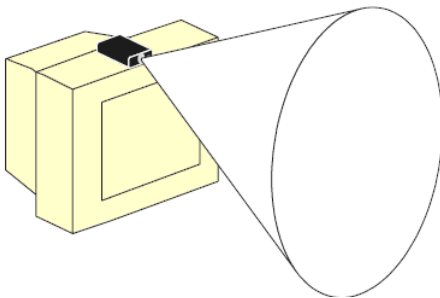
Nevertheless, pcProx-Sonar can be combined with building badges (RFID cards) to create a full-proof solution. The pcProx-Sonar, combined with building badge (RFID card) readers, gives us a low cost solution as compared to ARFID, which are expensive.

The device is attached to a computer via a USB port and is configured by the system as a keyboard. When a user walks away from the computer, the device sends keystrokes to the computer. Likewise, when a user approaches the computer, the device can be configured to send a different set of keystrokes to the computer. AccessAgent can be configured to intercept these keystrokes and perform appropriate actions, for example, to lock the computer.

The device uses 40 kHz ultrasonic sound waves (which has a high frequency inaudible for people). It can detect a proximity zone ranging from 5 inches to 5 feet. The user should be able to move around within the zone without triggering a walk-away event.



pcProx-Sonar



Conical detection zone

The currently supported sonar device is the RF IDEas pcProx-Sonar BSE-PCPRX-SNR.

The pcProx-Sonar should not be used with ARFID since ARFID is itself a presence detector. Any other supported authentication factors can be used with the pcProx-Sonar include:

- Password only
- RFID
- Fingerprint
- USB Key

The following are recommended policy settings for using pcProx-Sonar as a presence detector:

Policy ID	Value
pid_presence_detector_enabled	True, or 1 (Yes)
pid_presence_detector_walk_away_sequence	Ctrl, Alt, PgDn
pid_presence_detector_walk_away_action	4 (Lock computer)
pid_presence_detector_walk_away_not_logged_on_action	4 (Lock computer)
pid_presence_detector_walk_away_action_countdown_secs	5

If the walk-away keystrokes for the pcProx-Sonar is set to some other keystrokes, this policy should also be set accordingly.



The machine must be restarted for the above policy settings to take effect.

To install the sonar device:

- 1 Connect the pcProx-Sonar device to the computer.



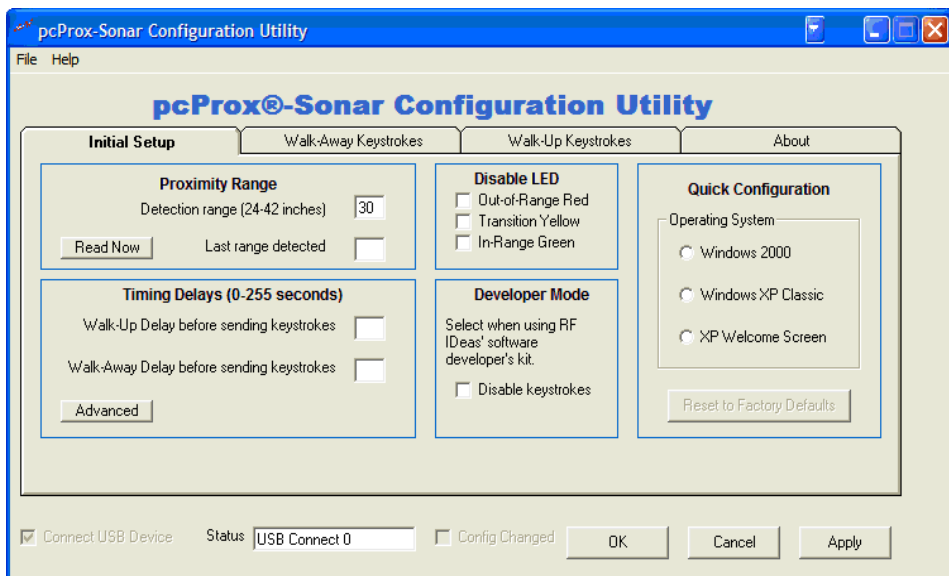
This device uses standard Windows built-in drivers and does not need any driver installation.

- 2 Launch the pcProx-Sonar Configuration Utility to configure the keystrokes sent by the device. Select the **Initial Setup** tab.

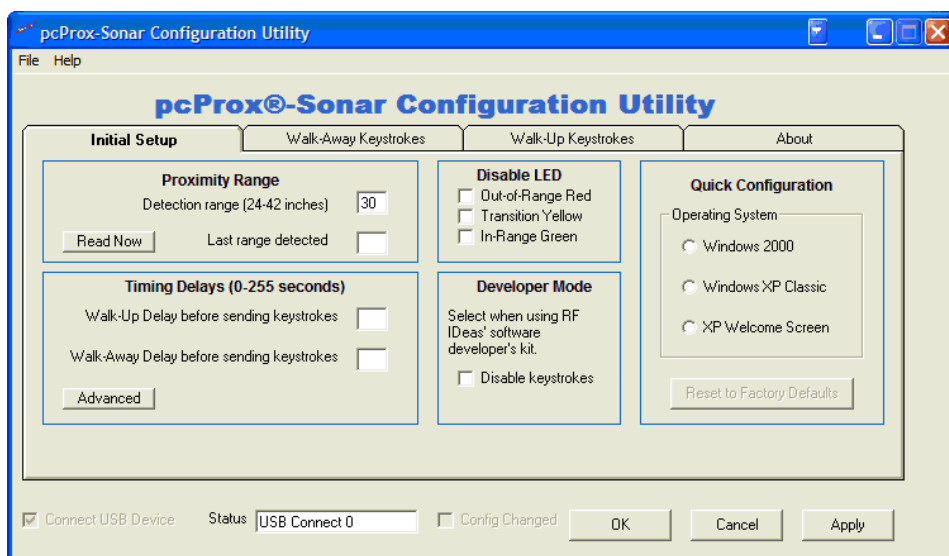


The software can be downloaded from <http://www.rfideas.com/html/downloads.html>.

- 3 Set the detection range in **Proximity Range** to **30 inches** (or other desired values).
- 4 Leave the **Timing Delays** as default.
- 5 Do not mark any boxes for Disable LED.
- 6 Do not mark the **Disable keystrokes** mode for Developer Mode.
- 7 Do not select any radio button for **Quick Configuration**.
- 8 In the **Walk-Away Keystrokes** tab, set **Keystroke 1** to **Ctrl, Alt, PGDN**, and set all the other keystrokes to **NONE**.



pcProx-Sonar Configuration Utility Initial Setup



pcProx-Sonar Configuration Utility Walk-Away Keystrokes

- 9 In the **Walk-Up Keystrokes** tab, set all the Keystrokes to **NONE**. As pcProx-Sonar cannot recognize a user and provide a user ID, the **walk-up** event is not currently supported by AccessAgent.



Other third-party software (either installed on the same computer AccessAgent is installed or elsewhere) may attempt to auto-configure the pcProx-Sonar device upon plug-in and send a different set of keystrokes for walk-away and walk-up. In such cases, AccessAgent cannot recognize the new keystrokes. Re-configure the keystrokes using the pcProx-Sonar Configuration Utility.

Active RFID

ARFID is both a second factor and a presence detector, as it can detect the presence of a user and AccessAgent can be configured to perform appropriate actions. See [Active RFID \(ARFID\)](#) for installation details and notes.

The following are recommended policy settings for using ARFID as a presence detector:

Policy ID	Value
pid_arfid_removal_action	4 (Lock computer)
pid_rfid_only_unlock_enabled	True, or 1 (Yes)



The presence detector policies (e.g., pid_presence_detector_enabled) are not applicable to ARFID.

PART II: INSTALLATION AND SETUP

Part II: Installation and Setup

Use this part of the guide to learn more about installing and setting up the main components of the Encentuate IAM Enterprise system. Refer to the following chapters:

- [AccessAgent Setup](#), which discusses how to install AccessAgent, customizing AccessAgent to your organization's needs, setting up automatic sign-on, and launching applications from EnGINA.
- [IMS Server Setup](#), which provides detailed instructions on setting up the server side of Encentuate IAM Enterprise, such as managing enterprise directories, installing IMS Server, improving IMS Server availability and scalability, and using AccessAdmin for administrative tasks.
- [Provisioning Setup](#), which provides an overview of the Provisioning API and the Encentuate Provisioning Agent.
- [Strong Authentication Setup](#), which offers useful tips on how to optimize an authentication tool's use and enhancing security for your organization.
- [AccessAssistant and Web Workplace Setup](#), which contains instructions on installing AccessAssistant and Web Workplace, managing system and user policies, and setting up automatic web sign-on for AccessProfiles.

AccessAgent Setup

This chapter covers the following topics:

- [Installing AccessAgent](#)
- [Setting up the IMS Server location](#)
- [Verifying the program folders and registry entries](#)
- [Changing the AccessAgent banner](#)
- [Setting a transparent screen lock](#)
- [Launching applications from EnGINA](#)
- [Setting automatic sign-on for Java applications](#)
- [Mapping network drives using EnWinNetUse](#)

Installing AccessAgent

The AccessAgent installer consists of the following:

- AccessAgent.msi
- Config folder
- Reg folder

The Config folder should contain the following:

- **DeploymentScript.vbs**: To be installed/executed
- **SetupHlp.ini**: Options to be used during installation
- **Any other file** (Example: **logon_banner.bmp**): To be copied to the Encentuate program files folder.



The uninstaller will not remove these copied files. These files will also not be repaired by the installer.

If `DeploymentScript.vbs` is used, make sure the VBScript contains the following:

```
sub PostCopy()  
  
end sub  
  
sub PreRemove()  
  
end sub
```

The script will be called after all the files have been transferred and registry has been written.

The Reg folder should contain the following:

- **DeploymentOptions.reg:** To be merged into the Windows registry
- Any other file will be ignored

The options provided in **SetupHlp.ini** are divided into 4 categories:

- **Setup time only options:** Options that cannot be changed after installation.
- **Setup time and runtime options that map to multiple registry values each:** Options that can be changed after installation (by modifying registry values), and each is mapped to several registry values.
- **Setup time and runtime options that map to one registry value each:** Options that can be changed after installation (by modifying registry values), and each is mapped to one registry value.
- **Dependency URLs:** URLs that installer directs user to if certain components required for installation are missing, for example, High Encryption Pack.

Option Name	Value	Description
EnginaEnabled	1 0 (default: 1)	Whether to replace current GINA with EnGINA. Note: For AccessAgent 3.3.0.0 and above, the behavior of this option is consistent for workstations, Terminal Servers, and Citrix servers. For Citrix servers, option 0 is recommended.
RebootEnabled	1 0 (default: 1)	Whether to trigger a machine reboot after setup.
RebootConfirmationEnabled	1 0 (default: 1)	Whether to confirm with user before rebooting. Effective only if RebootEnabled=1.
EnginaConflictPromptEnabled	1 0 (default: 1)	In case of GINA conflict, whether a prompt should be displayed.
UsbKeyPromptEnabled	1 0 (default: 1)	Whether to prompt user to insert USB Key, if it is not already inserted during installation time.
ImsConfigurationEnabled	1 0 (default: 1)	Whether to configure default IMS Server settings and install certificates from that server during setup.
ImsConfigurationPromptEnabled	1 0 (default: 0)	Whether to prompt user for the default IMS Server entry even if it is already correctly configured. Effective only if ImsConfigurationEnabled=1.
WalletCacheRemovedOnUpgrade	1 0 (default: 0)	Whether to remove cached Wallets on an upgrade.
InstallTypeGpo	1 0 (default: 0)	Whether to suppress all prompts and write to log. Required for AD GPO installation.
EncentuateRegistryRemovalEnabled	1 0 (default: 0)	Whether the Encentuate registry entries should be cleared after AccessAgent is uninstalled.
UsbKeyUtilityInstallationEnabled	1 0 (default: 0)	Whether to install the USB Key Utility when AccessAgent is installed.
EncentuateNetworkProviderEnabled	1 0 (default: 0)	Whether to enable the installation of Encentuate Network Provider during AccessAgent installation.

Setup time only options

Option Name	Value	Description
JVMInstallationDirectories	See description	Directories containing JVMs for which to enable Java automatic sign-on support. Each directory must be separated by a vertical bar. No space is allowed between two JVM directories. Example: "C:\Program Files\Java\jre1.5.0_11 C:\Encentuate\j2re1.4.1"

Setup time and runtime options that map to multiple registry values each

Option Name	Value	Description
ImsSecurePortDefault	default: 443	Default secure port number for the default IMS Server.
ImsDownloadPortDefault	default: 80	Default download port number for the default IMS Server.
ImsDownloadProtocolDefault	default: http://	Default download protocol for the default IMS Server.

Setup time and runtime options that map to one registry value each

Option Name	Value	Description
WalletTypeSupported	0: IMS only 1: Non-IMS only 2: Both IMS and non-IMS (default: 0)	Supported Wallet types.
ImsAddressPromptEnabled	1 0 (default: 1)	Whether to prompt user for IMS address during sign up, even if the IMS address specified in ImsServerName is correct.
ImsServerName	IMS Server hostname	Default IMS Server name.

The package of the **AccessAgent.msi** file, and **Config** and **Reg** folders can be centrally pushed out to client machines using software deployment tools like AD GPO or Microsoft Systems Management Server (SMS).

For certain push installations, you need to set the installer path in the **AccessAgent.msi** file as follows:

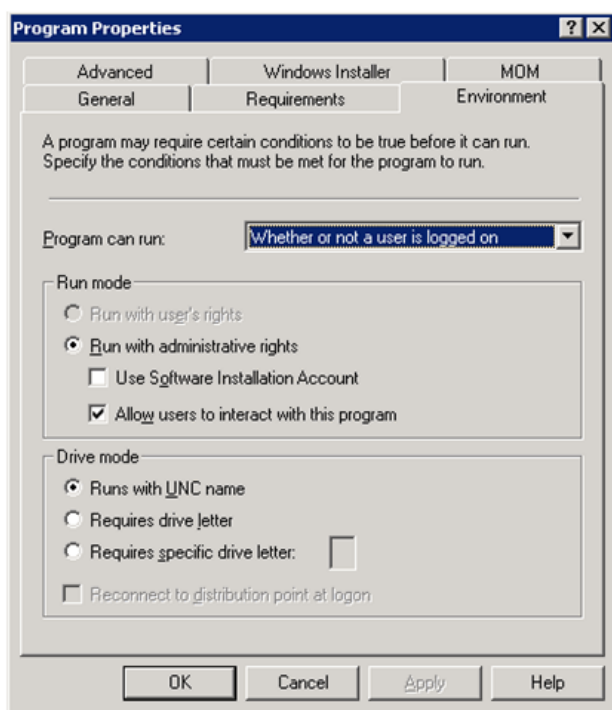
- 1 Open the **AccessAgent.msi** file using Orca editor (part of Windows Installer SDK).

- ❷ Click the **Property** table on the left.
- ❸ Set CONFIG_PARAMS_BASE_PATH to the desired path.

For deployment via SMS, especially during an upgrade, a VBScript can be written to present users with prompts such as, “You cannot use AccessAgent during the upgrade, such as, Single Sign-on to applications will be temporarily disabled. You will be prompted to restart the system when the upgrade is completed.”

This VBScript can then execute **AccessAgent.msi** with switches to suppress AccessAgent installer prompts (**AccessAgent.msi /q /norestart /1*v C:\AccessAgent.Log**). Select the **Allow users to interact with this program** check box under **Run mode** in the **Environment** tab of the **Program Properties** window to allow the VBScript to interact with the user with prompts.

If you cannot view or access the AccessAgent logs, it’s possible that the logs have been hidden for security purposes. Be sure that the policy **pid_log_obfuscation_enabled** is set to **No**.



:SMS Program Properties

To uninstall AccessAgent from a private desktop, refer to the deployment tip in [Uninstalling AccessAgent in private desktops](#) for more information.

Setting up the IMS Server location

The IMS Server location should normally be set during setup time by setting the **ImsServerName** key in **SetupHlp.ini** appropriately. The AccessAgent installer will automatically download the IMS Server certificate from the IMS Server.

If the downloading of the certificate fails during installation, the user will be prompted, the user can choose to proceed with the installation. However, the user cannot sign up or log on unless the certificate is successfully downloaded later.

This can be done by running *Start >> All Programs >> Encentuate AccessAgent >> Set IMS Server Location*. Alternatively, the same utility can be run by executing **C:\Program Files\Encentuate\SetupCertDlg.exe**.



*The Set IMS Server Location utility currently does not allow the user to modify the IMS Server name and port number. These will need to be modified by setting the registry entries that correspond to the appropriate machine policies: **pid_ims_server_name** and **pid_ims_download_service_port**.*

Verifying the program folders and registry entries

Program folders

The AccessAgent program files and data are stored, by default, within the **C:\Program Files\Encentuate** folder.

- **Program files:** C:\Program Files\Encentuate
- **Logs:** C:\Program Files\Encentuate\logs
- **User and machine Wallets (hidden files):** C:\Program Files\Encentuate\Cryptoboxes



*To see the Wallet files, make sure that Windows Explorer has been configured to **Show hidden files and folders**.*

The machine Wallet (**C:\Program Files\Encentuate\Cryptoboxes\Wallets\machine.wlt**) contains system policies and AccessProfiles downloaded from the current IMS Server. It is downloaded from IMS Server during the first startup after installation.

If the download of the machine Wallet is unsuccessful at startup, the synchronizer retries every 20 seconds for 5 times. After these 5 times, if downloading is still unsuccessful, the synchronizer will retry at intervals of 2 minutes until it is successful.



Since AccessAgent is installed to **C:\Program Files\Encentuate** by default, it assumes the presence of C: drive. Make sure that C: drive is present if the default installation folder is to be used.

Registry entries

AccessAgent registry entries are stored in the **[HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate]** key. Default registry values are automatically populated upon installation.

Machine policies are specified through registry values that are grouped under the appropriate registry keys according to the following convention:

Registry Key	Type of Policy
[Encentuate/IMSService/Default-IMSService]	Policies related to the default IMS Server
[Encentuate/DeploymentOptions]	All non-IMS machine policies
[Encentuate/IMSService/Global-IMSService]	URLs to SOAP services provided by IMS Server
[Encentuate/AccessAgent/Integration]	Settings related to integration with non-Encentuate software
[Encentuate/Temp]	Temporary registry values for development and troubleshooting purposes (these policies are not officially supported and should not be used for actual deployment)

Changing the AccessAgent banner

The banner on the AccessAgent user interface can be customized for customers.

To change the AccessAgent banner:

- 1 Prepare a bitmap file of size 432x64 pixels.



:Default AccessAgent Banner

- ② Name the file **logon_banner.bmp**.
- ③ Place the file in the installer's **Config** folder. The installer will automatically place the file in the Encentuate program files folder. If AccessAgent is already installed, the file can be manually placed in the Encentuate program files folder.

The banner should appear on the EnGINA welcome, on logon, lock/unlock windows, and the Desktop AccessAgent window.

Setting a transparent screen lock

For some deployments (e.g., manufacturing floor), the computer monitor is a status display for the machine tools and processes. They must remain visible at all times, so that any worker coming by can quickly scan all nearby monitors and alert someone when situation warrants.

For such cases, a transparent screen lock can be used instead of the normal Windows screen lock, which hides the current user's desktop. The transparent screen lock is essentially a transparent veil that covers the entire user desktop, so that the keyboard and mouse appear are disabled except for the Encentuate Hot Key, while the monitor still shows the full content of the Windows desktop.

The AccessAgent user interface that occupies the center of a locked screen will not be displayed. Instead, a small display indicates who is currently logged on and asks user to tap badge for unlocking at the Windows notification area. The user can tap an RFID badge or press the Encentuate Hot Key to unlock. Note that privacy considerations required elsewhere do not apply here.

When the transparent screen lock is active, the AccessAgent user interface is displayed when Encentuate Hot Key is pressed. The only options that will be presented to user are **Unlock this computer** and **Log off AccessAgent**. The latter allows user to manually log off AccessAgent, thereby unlocking the computer, and actions specified by **pid_logoff_manual_action** will be performed.

The following are recommended policy settings for transparent screen lock:

Policy ID	Value
pid_lock_option	2 (Transparent screen lock when AccessAgent is logged on, EnGINA screen lock otherwise)
pid_lock_transparent_text	Set to desired text that should be shown at the Windows notification area when transparent screen lock is activated. Default is "Tap your RFID card or Ctrl+Alt+E to unlock."

Policy ID	Value
pid_lock_transparent_hot_key_enabled	Set to 1 (Yes) if the Ctrl+Esc Hot Key sequence is to be enabled as an alternative to the Encentuate Hot Key during transparent screen lock. This additional Hot Key is useful for remote access systems (e.g., LANDesk) that can send only limited key sequences.
pid_enc_hot_key_enabled	True, or 1 (Yes)
pid_desktop_inactivity_action	4 (Lock computer)

Take note of the following:

- When transparent screen lock is activated, the monitor shows the full content of the Windows desktop.

If a user is logged on to AccessAgent and has opened several applications, anybody passing by can see the applications. This is acceptable provided that those computers are not used for any personal applications.

- The solution actually does not deactivate mouse or keyboard events.

The transparent screen simply does not react to any keyboard and mouse event. However, if some application running on the desktop displays some window and makes it the top most window later on, the application can receive the keyboard and mouse events.

- Transparent screen lock is only shown when computer is manually locked by the user from desktop, or when desktop inactivity is triggered.

The EnGINA screen lock will be shown if user attempts to enter a session through means where a normal computer lock screen would be shown, for example, logon using RDP. In such cases, it is possible for a user to see the transparent screen lock after unlocking the EnGINA screen lock.

- Even after transparent screen lock is activated, the action specified by **pid_desktop_inactivity_action** will still be carried out after a period of desktop inactivity has elapsed.
- With transparent screen lock enabled, **pid_locked_computer_inactivity_action** will not be effective since it is only applicable to EnGINA screen lock.
- With transparent screen lock enabled, unlock scripts (**pid_script_unlock_enabled**) will not be executed.
- Currently, sign up from transparent screen lock is not fully supported. If an unregistered RFID card is tapped, the user will be asked whether to log off the previous user, upon which the desktop will be unlocked and user will be brought into the sign-up workflow.

When transparent screen lock is invoked, it may be necessary to run a script to ensure that all applications are minimized except for the application that displays manufacturing status. Below is an example of such a VBScript that can be run as a lock script (**pid_script_lock_enabled**). When it's run, it minimizes all applications except the one with title "Calculator".

```
appTitle = "Calculator"

Set objShell = CreateObject("Shell.Application")

objShell.MinimizeAll

Set WshShell = CreateObject("WScript.Shell")

WshShell.AppActivate(appTitle)

WScript.Sleep 100

WshShell.SendKeys "% ( )"

Wshshell.Sendkeys "{ENTER}"
```

Launching applications from EnGINA

EnGINA (welcome and locked screen) can be configured to allow users to launch an application by clicking on a link in the left panel. This feature may be useful for the following scenarios:

- To allow users to launch AccessAssistant or Web Workplace (using Web browser) to perform self-service password reset.
- To allow users to launch a third-party application to perform self-service password reset or registration.
- To allow guest users to launch an application that is meant for public access without the need to log on to Windows.

The following are policy settings for enabling this feature:

Policy ID	Value
pid_engina_app_launch_enabled	1 (Yes)
pid_engina_app_launch_label	To be set to desired text that should be used as label for the application launch link, which will be shown in the left panel of EnGINA. For example, "Self-service password reset".

Policy ID	Value
pid_engina_app_launch_cmd	To be set to desired command line that will launch the application. For example, "C:\Program Files\Internet Explorer\iexplore.exe".



If the application is launched from the welcome screen, the owner of the process for the application will be "System". If the application is launched from locked screen, the owner of the process for the application will be "currently logged on desktop user".

The following command line can be used to launch AccessAssistant or Web Workplace using Internet Explorer in **kiosk** mode: **"C:\Program Files\Internet Explorer\iexplore.exe" -k https://preview.encentuate.com/WebWorkplace/reset_password_front_page.jsp.**

However, this method of launching applications have the following security issues:

- As the application will be launched in the context of "System" or "current logged on desktop user", the user may be allowed to access and modify files. For example, for Internet Explorer, the user can right-click on a graphic and select **Save Picture As...** to get a file explorer dialog box.
- The application may allow users to use features that are not intended for them. For example, for Internet Explorer, user can press **Ctrl+O** to open any file or **Ctrl+N** to open a new browser window.

As a workaround for the security issues, a Guest account with limited rights should be created and the application should be launched in the context of the Guest account. The Windows `runas` command can be used to launch the application in the desired user context.

However, since `runas` requires a password to be entered interactively, a script would have to be used to simulate keystrokes. The example VBScript (stored in the machine as **C:\launch_ie_as_guest.vbs**) as shown can be used to perform the application launch.

The script also sets the appropriate Internet Explorer feature restrictions for the Guest account. Machine policy **pid_engina_app_launch_cmd** should then be set to `cscript C:\launch_ie_as_guest.vbs`.

```
On Error Resume Next
```

```
userName = "Guest"
```

```
userDomain = "MOUNTCOOK"
```

```
userPasswd = "password"
```

```

appRunasCmd = "C:\Program Files\Internet Explorer\iexplore.exe
-k https://preview.encentuate.com/WebWorkplace/
reset_password_front_page.jsp"

appCmd = ""C:\Program Files\Internet Explorer\iexplore.exe" -
k https://preview.encentuate.com/WebWorkplace/
reset_password_front_page.jsp"

Set WshShell = CreateObject("WScript.Shell")

Set WshNetwork = WScript.CreateObject("WScript.Network")

currUser = WshNetwork.UserName

If currUser = "SYSTEM" Then

' Launched from EnGINA welcome screen as System context

' Optional: Set Internet Explorer restrictions for System user

regKey = "HKEY_USERS\S-1-5-
18\SOFTWARE\Policies\Microsoft\Internet Explorer\Restrictions\"

WshShell.RegWrite regKey & "NoBrowserClose", 0, "REG_DWORD"
'Allow user to close browser

WshShell.RegWrite regKey & "NoBrowserContextMenu", 1,
"REG_DWORD" 'Disable right-click menu

WshShell.RegWrite regKey & "NoFileOpen", 1, "REG_DWORD"
'Disable Ctrl-O to open file

WshShell.RegWrite regKey & "NoOpenInNewWnd", 1, "REG_DWORD"
'Disable Ctrl-N to open new browser

' Launch application in System context as there is no user
desktop

result = WshShell.Run(appCmd, 1, False)

Else

' Launched from EnGINA lock screen as user context

' Launch application using runas

```

```

Set WshEnv = WshShell.Environment("Process")

runasPath = WshEnv("SystemRoot") & "\System32\runas.exe"

result = WshShell.Run("runas /user:" & userDomain & "\" &
userName & " " & Chr(34) & appRunasCmd & Chr(34), 2, False)

WScript.Sleep 30 'Wait for cmd window to show up

WshShell.AppActivate(runasPath)

WshShell.SendKeys userPasswd & vbCrLf

' Optional: Set Internet Explorer restrictions

WScript.Sleep 1000 'Wait until user context loaded

Set wmiService =
GetObject("winmgmts:{impersonationLevel=Impersonate}")

Set wmiUserAccount = wmiService.Get("Win32_UserAccount.Name='" &
userName & "',Domain='" & userDomain & "'")

userSid = wmiUserAccount.SID

regKey = "HKEY_USERS\" & userSid &
"\SOFTWARE\Policies\Microsoft\Internet Explorer\Restrictions\"

WshShell.RegWrite regKey & "NoBrowserClose", 0, "REG_DWORD"
'Allow user to close browser

WshShell.RegWrite regKey & "NoBrowserContextMenu", 1,
"REG_DWORD" 'Disable right-click menu

WshShell.RegWrite regKey & "NoFileOpen", 1, "REG_DWORD"
'Disable Ctrl-O to open file

WshShell.RegWrite regKey & "NoOpenInNewWnd", 1, "REG_DWORD"
'Disable Ctrl-N to open new browser

End If

```

Setting automatic sign-on for Java applications

Use the target JVMs to configure AccessAgent to perform automatic sign-on for Java applications and applets. This can be done using the JVMInstallationDirectories installer option (see [Installing AccessAgent](#)) during installation.

If automatic sign-on is configured after AccessAgent is installed, perform the following steps for each JVM used to run Java applications and applets:

- ❶ Launch command prompt (*Start >> Run >> "cmd"*).
- ❷ Go to **JavaSupport** sub-folder of the Encentuate program directory (**cd C:\Program Files\Encentuate\JavaSupport**).
- ❸ Execute **JSupportInstaller.bat** with the installation directory of the JVM as its argument (e.g., **JSupportInstaller.bat "C:\Program Files\Java\j2re1.4.2_08"**).



This batch file must be started from the "JavaSupport" sub-folder of the Encentuate program directory.

Mapping network drives using EnWinNetUse

On shared workstations using generic accounts for Windows logon, it may be necessary to map user-specific network drives when a user logs on to AccessAgent. **EnWinNetUse.exe** is an application that can be used to achieve that. It is installed together with AccessAgent and can be found in the Encentuate Program Files directory.

Usage

```
EnWinNetUse.exe [-d <drive letter(s)>] [-p <network path(s)>]  
[-u <user name>] [-x <domain>] [-r] [-v] [-s]
```

- **-d:** A drive letter or list of drive letters. Note that a drive can either be specified as a letter that is not in use (e.g., "J:" – note that ":" is required), or simply use "*" to have the drive letter automatically assigned. If there are multiple network drives that to be mapped, each of them must be separated by a "/" character. No space is allowed. The number of network drives and the network paths specified must be the same and have one-to-one correspondent relationship. If they are not the same, the smaller list will be effective. If an error occurs when mapping one drive, other drives will be continued to be mapped.
- **-p:** A network path or list of network paths. If there are multiple network drives that to be mapped, each of them must be separated by a "/" character. No space is allowed (unless space is part of the file or folder name). The number of network drives and the network paths specified must be the same and have one-to-one correspondent relationship. If they are not the same,

the smaller list will be effective. If an error occurs when mapping one drive, other drives will be continued to be mapped.

- **-u:** User name to be used for mapping the drives.
- **-x:** Domain to be used for mapping the drives.
- **-r:** Remember network drive connections.
- **-v:** For verbose error messages.
- **-s:** Use simplified user interface (only showing user name, password, and domain).

To configure AccessAgent to use EnWinNetUses:

- ❶ Configure the AccessAgent logon script to launch **EnWinNetUse.exe** with appropriate parameters (set the following policies accordingly:
pid_script_logon_enabled, pid_script_logon_type, pid_script_logon_code)
- ❷ Using AccessStudio, create an AccessProfile for EnWinNetUse, so that the appropriate Windows credentials can be auto-filled in the EnWinNetUse prompt.
- ❸ When the user logs on to AccessAgent, **EnWinNetUse.exe** will be launched by the AccessAgent logon script. Windows credentials are then auto-filled by AccessAgent, allowing **EnWinNetUse.exe** to map the drives accordingly for the user.

IMS Server Setup

After installing IMS Server, IMS Server uses the base connector for Encentuate user validation. Any user can sign up as a new Encentuate user without providing validation credentials.



For IMS Server upgrades, the existing settings (e.g., Java Virtual Machine, concurrent threads, etc.) are not affected. These settings are retained and do have to be reconfigured.

To use Active Directory or some other enterprise authentication services to validate users during sign up, you must configure the authentication service for user validation using the IMS Configuration Utility. This should be complete before IMS Server is available to users for signing up.

Refer to the Encentuate IAM Administrator Guide for instructions on installing the IMS Server.

This chapter covers the following topics:

- [Using the IMS Configuration Utility](#)
- [Enterprise directory setup](#)
- [Preparing the IMS database](#)
- [Improving IMS Server performance](#)
- [Managing IMS clusters](#)
- [Using AccessAdmin](#)
- [Role assignment features](#)
- [Managing remote access for IMS Servers](#)

Using the IMS Configuration Utility

The IMS Configuration Utility provides professional services with a user interface for configuring the IMS configuration keys (in **<IMS Installation Folder>\ims\config\ims.xml**).

The utility is installed, by default, on port 8080 and can only be accessed locally from the server console, for security reasons (URL: `http://<server-name>:8080/`). It can be accessed from the Start Menu through *Start >> Programs >> IMS Server >> IMS Configuration Utility*. Unlike AccessAdmin, the utility does not authenticate users

The IMS Configuration Utility is only available when IMS Server is running. Since IMS Server loads the configuration keys on startup, it is necessary to Restart the IMS Server after any configuration is done through the utility, so that the configuration can take effect:

- Stop the IMSService (`net stop IMSService`).

Start the IMSService (`net start IMSService`) or run the batch file: **<IMS Installation Folder>\ims\bin\runserver.bat**.

Enterprise directory setup

Use an enterprise directory to manage user accounts, including those maintained by the IMS Server. The topics included in this main topic provide instructions on setting up new enterprise directories, an ADSI application connector, an active directory forest, and other application connectors.

Enterprise directories are set up using the IMS Configuration Utility. After installing IMS Server, the IMS Configuration Utility is automatically launched with the Active Directory (ASD) configuration wizard. Specify the following in the wizard to configure Active Directory as enterprise directory.

- **DNS Domain Name**

The DNS domain name of the Active Directory that IMS Server should connect to (e.g., **domain.encentuate.com**).

- **Lookup User Name**

User name of the Active Directory user that IMS Server will use to obtain attributes of all users throughout the Active Directory forest. This lookup user should have appropriate rights.

- **Lookup Password**

Password of the Active Directory lookup user.

■ Use Active Directory password as Encentuate password

Mark this checkbox if the Encentuate password synchronizes with the Active Directory password (such as, enable Active Directory password synchronization). Clear this checkbox if users do not synchronize Encentuate passwords with the Active Directory passwords.

About enterprise directories

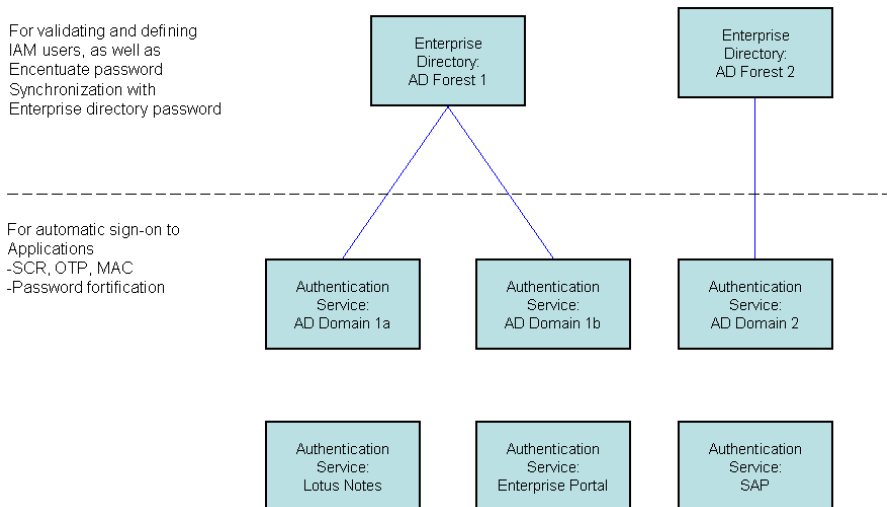
An enterprise directory is an entity that validates user credentials for Encentuate IAM Enterprise users. It can be used for validating users during signup and also during login, if the Encentuate password is set up to synchronize with the enterprise directory password. In short, it is a directory of user accounts that define Encentuate IAM Enterprise users. An example of an enterprise directory is an Active Directory forest.

An enterprise directory may contain zero or more authentication services. An Active Directory forest with multiple domains can be an enterprise directory that contains multiple authentication services, with each authentication service representing one domain. Such a definition, coupled with the password synchronization feature, allows enterprise directory passwords to be used for both logon to Wallet and automatic sign-on to applications.



For simplicity purposes, an authentication service is always automatically created by the IMS Configuration Utility when an enterprise directory is created. This authentication service can be ignored if it is not used for application authentication.

The concepts are summarized in the following diagram:



Enterprise directory structure

A connector should be defined for each enterprise directory, so that the IMS Server can communicate with it. The IMS Server will use the connector during sign-up or login, to validate each user's credentials.

The connector is also used for searching the enterprise directory and for obtaining user attributes, such as email, phone number, etc. This same connector is automatically applied to all authentication services (Active Directory domains) that belong to the enterprise directory, making it easier to create and maintain connectors for multiple Active Directory domains.

With the enterprise directory defined, Encentuate IAM Enterprise can identify a user by an UPN (e.g., **bob@encentuate.com**, where "encentuate.com" may not be the same as the Active Directory domain name). This is because UPNs are unique across an Active Directory forest, and the Active Directory forest is represented in Encentuate IAM Enterprise by an enterprise directory.

Provided both the enterprise directory and the UPN are known, Encentuate IAM Enterprise can uniquely identify the user. This feature reduces the learning curve for users as it retains part of the look and feel, and behavior of the Windows logon prompt.

An authentication service was used to specify any entity that validates user credentials. It was used for automatic sign-on, where each set of application user names and passwords were tied to some authentication service. It was also used for validating users during sign-up.



For example, the Active Directory domain could be defined as the authentication service for validating users. With the enterprise directories feature, an enterprise directory is now used for validating and defining Encentuate IAM Enterprise users, whereas an authentication service will continue to be used for validating application credentials. The separation of these two concepts is necessary because a single enterprise directory may actually provide multiple authentication services.

Setting up a new enterprise directory

If Active Directory is not the enterprise directory or advanced settings need to be configured, they can be set up using the IMS Configuration Utility.

To set up a new enterprise directory:

- ❶ Go to the IMS Configuration Utility (*Basic Settings >> Enterprise Directories*). Click **Add Directory** to add a new enterprise directory.
- ❷ Specify the following settings for the new enterprise directory.

Enterprise Directory ID

This field is specified by the Administrator, and represents the unique ID of the enterprise directory. It can be any name specified by the Administrator.

Enterprise Directory Name:

This field assigns a name to the enterprise directory, and is specified by the Administrator.



This will be used as the enterprise directory's display name.

Description

This field contains a description of the enterprise directory.

Synchronize user password with the password in the enterprise directory?

Select **Yes** if the Encentuate password will synchronize with the enterprise directory password (if enterprise directory is Active Directory, this will be Active Directory password synchronization). Select **No** if users will use Encentuate passwords but not synchronize with the enterprise directory passwords.

Authentication Service Groups of the generated authentication services:

DomainAuthenticatorGroup (authentication service group for Windows authentication) must be selected in this field.



This field must be modified if you have created other authentication service groups for Windows authentication.

Link with existing authentication service (directory ID/DNS domain name: authentication service ID)

This field is important when upgrading IMS Server. It maps the DNS domain name of each Active Directory domain with existing authentication services. Specify the DNS domain names and authentication service IDs in the specified format (e.g., encentuate.com:dir_encentuate_domain). Leave this field blank for fresh IMS Server installations.

Included in the enterprise directory list for Encentuate users validation?

Mark this checkbox if this enterprise directory will be set as the enterprise directory for validating Encentuate users. Currently, only one enterprise directory is allowed in the list. If there is already an enterprise directory in the list, it will be replaced by the new enterprise directory.

- ③ Once all the above fields have been configured, click **Add**.

Setting up an ADSI application connector

- 4 Specify information for the new ADSI application connector.

Application Connector

Select **Active Directory (ADSI) Connector**, then click **Configure**. This connector is recommended as it supports multiple forests. To use other types of connectors, see [Setting up other application connectors](#).

Specify the domain type to be shown in AccessAgent

Set to NetBIOS to be consistent with the Windows logon interface.

- 5 To add an Active Directory forest, click **Add Forest**.

Setting up an Active Directory (ADSI) Forest

- 6 Specify information for the new Active Directory forest.

Forest Name

This is specified by the Administrator, and it represents the name in which the forest will be identified.

Active Directory Server URI

Specify the Active Directory server that IMS Server should connect to (e.g., adserver.encentuate.com). This should be the hostname of the Active Directory server, followed by the domain DNS name.

For example, if the hostname of the Active Directory server is "adserver", and the domain DNS name is "encentuate.com", then you should use "adserver.encentuate.com" for this field. Some deployments may have multiple Active Directory servers for redundancy.

To use the Active Directory server redundancy, the IMS Server OS should join the same forest. Indicate the domain controller DNS name in the Active Directory Server URI configuration. IMS Server will then automatically use the Active Directory server redundancy.

Note that the enterprise DNS must be set up so the domain DNS name can be resolved correctly at IMS Server and all client machines. If not, user sign-up may fail.

Lookup User Name

Specify the user name of the Active Directory user used by the IMS Server to obtain attributes of all users throughout the Active Directory forest. This user should have appropriate access rights. In a multi-domain configuration, the lookup account should be specified in "domain\username" format.



For IMS Server 3.3.1.4 and above, the domain part can be omitted only if the lookup account is in the same domain as the user which the IMS service impersonates.

Lookup User Password

Enter the password of the Active Directory lookup user.

LDAP User Tree DNs

This field allows the Administrator to add and remove user trees to and from the Active Directory forest. Each user tree should be entered in the specified format (e.g., **CN=Users,DC=encentuate,DC=com**). Users who belong to trees but not specified here will not be searchable and will not be allowed to sign up.



These user trees must be unique across forests. Two forests configured here cannot contain the same user tree DN. Use the Windows command-line utility dsquery.exe to obtain DNs.

- 7 After all the trees are added, click **Add** to add the Active Directory forest.
- 8 If there are no more changes, click **Test Connector** to make sure that all the settings are correct, then click **Save All**.

If errors occur when **Test Connector** is clicked, refer to the Microsoft knowledge base for the returned error code.
- 9 To create more forests, click **Add Forest** again, and perform the above configurations.

Setting up other application connectors

The Active Directory (ADSI) Connector is recommended for connecting to Active Directory as it supports multiple forests. However, if the enterprise directory is not an AD, other types of connectors can be used. The available connectors are as follows:

- **Active Directory (ADSI) Connector:** To connect to Active Directory using ADSI.
- **Active Directory (LDAP) Connector:** To connect to Active Directory using LDAP. To use this connector, LDAP must be enabled on Active Directory.
- **Always Allow Users Connector:** To allow users to sign up without authenticating to an enterprise directory.

- **Always Deny Users Connector:** To disallow users from signing up.
- **Generic LDAP Connector:** To connect to a generic LDAP server, including ADAM. The ADAM connector can only support two operations: verify user password, and get user attributes. An enterprise directory can also be configured to connect to either Active Directory or ADAM, but not at the same time.
- **NIS Connector:** To connect to NIS.
- **Windows NT Connector:** To connect to Windows NT server.

The next paragraphs describe the LDAP connector (Active Directory, generic, or ADAM) configuration. For tips regarding the configuration of the ADAM server, refer to [Configuring the ADAM Server](#).

Basic configuration keys

- **LDAP server URI:** The location of the LDAP server (e.g., `ldap://ldapserver-name:50001`).
- **Lookup user name:** The user name that has permissions for lookup operations. If not set, the LDAP server must support anonymous connections.
- **Lookup user password:** The corresponding password for the user name that has permissions for lookup operations.
- **Lookup user LDAP base DN:** The base distinguished name (DN) of the lookup user (e.g., `cn=users,o=encentuate,c=sg`).
- **LDAP User Tree DNs:** The distinguished names (DNs) of the users in the LDAP server (e.g., `cn=users,o=encentuate,c=sg`).
- **LDAP users DN attribute:** The distinguished name (DN) attribute for the users (e.g., `cn`).
- **LDAP lookup timeout:** The maximum time (in milliseconds) before an LDAP connection times-out.

Advanced configuration keys

- **Enterprise account LDAP attribute:** The LDAP attribute of the user for binding an IMS identity to an enterprise account (e.g., `cn`).
- **LDAP context factory:** The fully-qualified class name of the factory class that will create an initial context (e.g., `com.sun.jndi.ldap.LdapCtxFactory`). This configuration is optional.
- **LDAP security protocol:** The protocol used to connect to the LDAP server. The value should be `SSL` if the connector changes passwords, otherwise set it to `none`.

- **LDAP authentication type:** The authentication mechanism to use. Currently the use of **simple** is supported, which refers to user name and password.
- **LDAP referral:** Specifies how referrals returned by the LDAP server are processed. A value of **follow** means IMS Server follows referrals automatically. **ignore** means IMS Server ignores referrals. This configuration is optional.
- **LDAP password attribute:** The password attribute of each user on the LDAP server (e.g., **userPassword**).
- **LDAP search scope:** The scope for user search on the LDAP server. This field can be used to specify whether to search users on a single level of the LDAP tree or the entire sub-tree.
- **LDAP logins count limit:** The maximum number of user logins retrieved from the LDAP server when searching for users.
- **LDAP auto-deprovision action:** The deprovisioning action to use when automatic deprovisioning is done.
- **LDAP auto-deprovision method:** The deprovisioning method performed when a user is revoked. Possible values are **manual**, **automatic**, **none**, and **exclude**. For **exclude**, the account data is not copied to the revoked accounts table. For all other values, they are copied with the status set to the corresponding value. The default value is **exclude**.
- **LDAP Administrator user name:** A user name with Administrator privileges on the LDAP server. This user will be used to perform automatic deprovisioning.
- **LDAP administrator user password:** The password of the user with Administrator privileges on the LDAP server.

For IMS Server versions before 3.5, make sure that IMS Server settings are configured properly. Go to *Advanced Settings > > IMS Server*, and expand the *Miscellaneous* section.

If **#1 Single enterprise directory** (for backward compatibility) is selected, all user names must be unique, across domains and even forests. This mode is for backward compatibility with previous AccessAgent versions. In this mode, Active Directory domain need not be specified for logon and user search.

If user names may be duplicated across different domains, then **#2 Enable multiple enterprise directories and domains** should be selected.

When changing from #1 to #2, the Administrator must run the **upgradeAdUsers.bat** CLT, and Restart the IMS Server. You cannot change from #2 back to #1.



Only option #2 is supported from version 3.5 onwards. Resetting the option to #1 if there are duplicate names across the forests may cause unpredictable behavior. Only the user with the same user name may be able to sign up, but migration of this user may fail should this option be changed to #2.

Preparing the IMS database

The IMS database can be separately installed and prepared, or installed as part of the IMS installer after version 3.4.0.0. The supported databases are listed in [Minimum system requirements](#).

Should the IMS database and IMS Server be running on different machines, we recommend that the system clocks be synchronized. This can be achieved through the use of the time synchronization feature of Microsoft Windows that is based on Network Time Protocol (NTP). More information on the time synchronization feature of Windows can be found at:

- Windows 2000: <http://support.microsoft.com/kb/224799>
- Windows XP: <http://support.microsoft.com/kb/307897>
- Windows Server: <http://support.microsoft.com/kb/816042>

If the IMS database is manually prepared, it must satisfy the pre-requisites indicated in the following sections if IMS Server version is above 3.4.0.0.

Prerequisites for Microsoft SQL Server 2000

- Microsoft SQL Server 2000 (Standard, Enterprise, or Desktop Edition) with Service Pack 3.
 - SQL Server Authentication should be enabled. This can be done by using the SQL Enterprise Manager: Right-click *DB Server* >> *Click on Security tab* >> *Choose SQL Server and Windows authentication*.
 - The SQL Server should have TCP connections, SQL Server Authentication enabled. This can be done using the SQL Enterprise Manager: Right-click *DB Server* >> *Click on General tab* >> *Click Network Configuration button* >> *Enable TCP/IP and Named Pipes*.
 - If a named instance is used, the name of the instance and the port that the instance is running on should be known. You can check the port number by using the SQL Enterprise Manager: Right-click *DB Server/instance* >> *Click on General tab* >> *Click Network Configuration button* >> *Select TCP/IP* >> *Click properties*.
 - Disable all default connection options. This can be done by using the SQL Enterprise Manager: Right-click *DB Server* >> *Click on Connections tab* >> *Uncheck all Default connection options*.
- Administrator (SA) account and password for Microsoft SQL Server.

- For Administrator-created database, note that the Database collation should be SQL_Latin1_General_CP1_CS_AS.
- For Administrator-created database user, note that the user should have public, db_owner rights for the created database. The user should not be a DB Administrator account.

Prerequisites for Microsoft SQL Server 2005

- Microsoft SQL Server 2005 (Standard, Enterprise, or Express Edition) with Service Pack 1.
 - SQL Server Authentication should be enabled (SQL Server Management Studio: Right-click *DB Server* >> *Click on Security on the left panel* >> *Choose SQL Server and Windows Authentication mode*).
 - The SQL Server should have TCP connections, SQL Server Authentication enabled (SQL Server Configuration Manager: Click on *SQL Server Network Configuration* >> *Protocols* >> *Double-click TCP/IP* >> *Click the Protocol tab* >> *Set Enabled to Yes*).
 - Choose a static port for TCP connections (SQL Server Configuration Manager: Click on *SQL Server Network Configuration* >> *Protocols* >> *Double-click TCP/IP* >> *Click the IP Addresses tab* >> *Blank out all TCP Dynamic Ports* >> *Fill in all TCP Ports with 1433/any available static port*).
 - If a named instance is used, the name of the instance should be known.
 - Disable all default connection options (SQL Server Management Studio: Right-click *DB Server* >> *Click on Connections in the left panel* >> *Uncheck all Default connection options*).
- Administrator (SA) account and password for Microsoft SQL Server.
- For Administrator-created database, note that the Database collation should be SQL_Latin1_General_CP1_CS_AS.
- For Administrator-created database user, note that the user should have public, db_owner rights for the created database. The user should not be a DB Administrator account.

Prerequisites for Oracle

- Oracle 9i/10g Database with an instance created for IMS Server.
- Administrator (DBA) account and password for this instance, to be used by IMS Server.

Improving IMS Server performance

For new IMS Server installations, a typical number of concurrent connections can be handled. This is because IMS Server installations work out-of-the-box for typical small enterprises, POCs, and demos, without any need for configuration changes.

However, for larger enterprises, it is necessary to fine tune the performance parameters to meet the load requirements of each deployment. Failure to configure the performance parameters appropriately may cause IMS Server to be unresponsive to connection requests when the load is high.

Currently, the IMS installer always sets the memory allocation and connection parameters to default values on each installation or upgrade. It is necessary to perform the configuration steps in [Increasing the number of concurrent users](#) after every upgrade.

The IMS Server performance tuning parameters can be classified into four types:

- **Memory allocation:** The amount of RAM allocated to IMS Server.
- **Connection parameters:** The number of concurrent connections to be accepted or processed.
- **Database parameters:** Database pool size and time-out values.
- **RADIUS parameters:** The number of concurrent RADIUS requests to be accepted.

The optimal values of these parameters depend on a lot of external factors, which are different across deployments:

- Number of concurrent AccessAgent connections to IMS Server.
- Whether IMS Servers are load-balanced.
- Tasks performed on IMS Server (e.g., a deployment using OTP authentication may require more CPU power).
- CPU speed of IMS Server.
- Amount of physical RAM that can be allocated to IMS Server.
- Whether the database server is sharing the same machine with IMS Server.
- CPU speed of database server.
- Amount of physical RAM allocated to database server.
- Capability of the database server (e.g., number of concurrent connections it can handle).

- Quality of the network (e.g., slow network requires higher time-out thresholds for database connections).

Memory allocation parameters are listed in the next table. These parameters specify the amount of memory allocated to the JVM.

Refer to the JVM Documentation for more information: <http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/java.html>

Parameter Name	Description	Default Value
-Xmx	<p>The maximum size (in bytes) of the memory allocation pool. This value must a multiple of 1024 greater than 2MB. Append the letter k or K to indicate kilobytes, or m or M to indicate megabytes. Based on load testing results, the recommended value for this configuration parameter is 512MB. This is assuming that the server has at least 1GB of RAM. Examples are: -Xmx83886080, -Xmx81920k, and -Xmx80m</p> <p>Note: <i>There is no space between the switch and its value.</i></p>	128m
-Xms	<p>The initial size (in bytes) of the memory allocation pool. This value must be a multiple of 1024 greater than 1MB. Append the letter k or K to indicate kilobytes, or m or M to indicate megabytes. The default value is 2MB. Examples are:-Xms6291456, -Xms6144k, and -Xms6m</p> <p>Note: <i>There is no space between the switch and its value.</i></p>	24m
-Xss	<p>The thread stack size. This parameter need not be modified unless there are a lot of recursive functions or deep method-call-stacks.</p>	1024k

Connection parameters are listed in the next table. These parameters control the number of concurrent AccessAgent connections IMS Server can handle. With default values (see table below), IMS Server can only handle 175 concurrent users at most, while 75 of them can be serviced at the same time and 100 waiting to be serviced. Any additional requests will be rejected.

AccessAgent has a machine policy setting (**pid_net_soap_timeout_secs**) that indicates the number of seconds to wait before connection time-out. The default value is 20 seconds. It should be no less than the **connectionTimeout** parameter below.

Refer to the Apache Tomcat 4 Configuration Directives for more information: <http://tomcat.apache.org/tomcat-4.1-doc/config/index.html>

Parameter Name	Description	Default Value
minProcessors	<p>Specifies the number of request processing threads that will be created when IMS Server is first started.</p> <p>Specifies the maximum number of request processing threads to be created by IMS Server, which therefore determines the maximum number of simultaneous requests that can be handled.</p> <p>Based on load testing results, the following are recommended values for this configuration parameter:</p> <p>If RADIUS authentication (for OTP) is used, set this to 700.</p> <p>If RADIUS authentication (for OTP) is not used, set this to 1000.</p> <p>The above recommended values are based on the assumption that the server has at least 1 GB of RAM.</p>	75
acceptCount	<p>Specifies the maximum queue length for incoming connection requests when all possible request processing threads are in use. Any requests received when the queue is full will be refused.</p>	100
connectionTimeout	<p>Specifies the number of milliseconds IMS Server will wait, after accepting a connection, for the request URI line to be presented.</p>	20000

Database parameters are listed in the next table. Note that there are separate configurations for connections to the IMS database (which stores system data, user passwords, etc.) and the IMS log database (which stores audit logs), although most of the time, the IMS database and log database reside on the same database server.

The maximum database pool sizes (**ds.ims.rdb.pool.maxsize** and **ds.ims_log.rdb.pool.maxsize**) should be comparable to the sum of the connection parameter **maxProcessors** and RADIUS parameter **radius.maxPackets**. This is because each connection from AccessAgent or RADIUS request usually requires a database connection.

The database connection time-out values (**ds.ims.rdb.pool.maxwait** and **ds.ims_log.rdb.pool.maxwait**) should not be larger than the connection parameter **connectionTimeout** or the AccessAgent machine **policy pid_net_soap_timeout_secs**.

Parameter Name	Description	Default Value
ds.ims.rdb.pool.maxsize	Specifies the maximum number of concurrent database connections to IMS database.	50
ds.ims.rdb.pool.maxwait	Specifies the maximum number of milliseconds a connection to IMS database waits before it times out.	5000
ds.ims_log.rdb.pool.maxsize	Specifies the maximum number of concurrent database connections to IMS log database.	50
ds.ims_log.rdb.pool.maxwait	Specifies the maximum number of milliseconds a connection to IMS log database waits before it times out.	5000

RADIUS parameters are listed in the table below. Note that this setting is only required if the RADIUS authentication feature of IMS Server is used.

Parameter Name	Description	Default Value
radius.maxPackets	Specifies the maximum number of concurrent RADIUS packets the server will handle. Based on load testing results, the recommended value for this configuration parameter is 400. This is assuming that the server has at least 1 GB of RAM.	1000

Optimizing memory for the IMS Server

For new installations, the IMS Server is allocated only a maximum of 128MB of RAM. Should more memory be allocated to the server, perform the following operations:

- Edit the Java Virtual Machine and Tomcat **-Xmx** and **-Xms** options in **run-server.bat**:
 - Edit the file **<IMS Installation Folder>\ims\bin\runserver.bat**.
 - By default, the line that contains the **-Xmx** and **-Xms** options look like this:
set JAVA_OPTS=-Xmx128m -Xss1024k -Xms24m.....
 - To change the memory allocation to, say, 512MB, edit the line accordingly:
set JAVA_OPTS=-Xmx512m -Xss1024k -Xms512m.....

- Save the edited file.
- Edit the Java Virtual Machine and Tomcat **-Xmx** option in `installService.bat`:
 - Edit the file **<IMS Installation Folder>\ims\bin\installer\installService.bat**.
 - By default, the line that contains the **-Xmx** and **-Xms** options look like this:
set JAVA_OPTS=-Xmx128m -Xss1024k -Xms24m.....
 - To change the memory allocation to, say, 512MB, edit the line accordingly:
set JAVA_OPTS=-Xmx512m -Xss1024k -Xms512m.....
 - Save the edited file.
 - After modifying `installService.bat`, you need to run it once such that those new settings take effect the next time IMS Service is started. To run the batch file, go to the **<IMS Installation Folder>\bin\installer** folder and run **installService.bat** ~~change~~**it** in command line.

The IMS Server must be restarted for the new configurations to take effect. Note that it is necessary to perform all the above configuration steps after every upgrade.

Increasing the number of concurrent users

For new installations, IMS Server can only handle 175 concurrent users at most, while 75 of them can be serviced at the same time and 100 waiting to be serviced. Any additional requests will be rejected. Should more concurrent connections be handled, perform the following operations:

Edit the connection parameters in **server.xml**:

- Edit the file **<IMS Installation Folder>\conf\server.xml**.
- Modify the parameters below to the appropriate values.

```
<Connector
className="org.apache.coyote.tomcat4.CoyoteConnector"

    port="80" minProcessors="5" maxProcessors="75"
    enableLookups="false" redirectPort="443"
    acceptCount="100" debug="0" connectionTimeout="20000"
    useURISValidationHack="false" disableUploadTimeout="true" />

<Connector
className="org.apache.coyote.tomcat4.CoyoteConnector"

    port="443" minProcessors="5" maxProcessors="75"
    enableLookups="false"
    acceptCount="100" debug="0" scheme="https" secure="true"
    useURISValidationHack="false" disableUploadTimeout="true">
```



```
<Factory className="encentuate.tomcat.SslSocketFactory"

    clientAuth="false" protocol="TLS"
    keystoreFile="ims/certs/keystore/ssl_keystore"
    keystorePass="*****" />

</Connector>
```

- Save the edited file.

The IMS Server must be restarted for the new configurations to take effect. Perform all the above configuration steps after every upgrade.

Increasing the database connection pool size

For new installations, the IMS Server is only allocated a maximum database connection pool size of 50 each for the IMS database and log database. Should the maximum database connection pool sizes and connection time-out values be modified, perform the following operations:

- ① Launch IMS Configuration Utility.
- ② Go to *Advanced Settings >> Data Source >> IMS Data Source*.
- ③ Modify the parameter **Maximum Connection-Pool Wait In MilliSeconds** accordingly. This is the database parameter **ds.ims.rdb.pool.maxwait**.
- ④ Modify the parameter **Maximum Connection-Pool Size** accordingly. This is the database parameter **ds.ims.rdb.pool.maxsize**.
- ⑤ Go to *Advanced Settings >> Data Source >> Log Data Source*.
- ⑥ Modify the parameter **Maximum Log Connection-Pool Wait In MilliSeconds** accordingly. This is the database parameter **ds.ims_log.rdb.pool.maxwait**.
- ⑦ Modify the parameter **Maximum Log Connection-Pool Size** accordingly. This is the database parameter **ds.ims_log.rdb.pool.maxsize**.

The IMS Server must be restarted for the new configurations to take effect.

Increasing the maximum number of RADIUS packets

For new installations, the IMS Server is configured to handle a maximum of 1000 concurrent RADIUS packets. Should this value need to be modified, perform the following operations:

- ❶ Edit the **ims.xml** file, which should be found in **<IMS Installation Folder>\ims\config**.
- ❷ To change the **radius.maxPackets** parameter to add the following configuration key (e.g. 400):

```
<radius.maxPackets>  
  
<value xml:lang="en">400</value>  
  
</radius.maxPackets>
```

- ❸ Save the modified **ims.xml** file.

The IMS Server must be restarted for the new configurations to take effect.

Enhancing server scalability and availability

Scale up:

- Enhance CPU hardware (faster CPU or multi CPU) since database server is CPU-intensive.
- Add more RAM since database server is also memory-intensive.

Scale out:

- Limited in capability and vendor dependent.
- Microsoft SQL Server 2000 Clustering is primarily for enhanced availability, not enhanced scalability. The scalability solution, Distributed Partitioned Views, requires careful partitioning of data across two or more separate databases, and is not supported by IMS Server.
- Oracle Clustering (ORAC) allows scaling to multiple nodes.

High Availability:

- Microsoft SQL Server 2000 Clustering involves two nodes in Active-Passive mode. It allows two servers to share a set of resources (e.g., disks) and services/applications, but only one server is actively serving users at any time. It runs on top of the Microsoft Clustering Service.

- Oracle Clustering is in Active-Active mode, such as, all nodes can be actively serving users at the same time. It involves shared access to disk and uses the CacheFusion technology that has a special Memory Interconnect link between servers to synchronize the database cache in each server.

High availability setup (HA) for the database tier typically involves:

- Need for shared external SCSI Disk Array.
- Expensive edition of OS: Enterprise Edition instead of Standard Edition.
- Expensive edition of database: Enterprise Edition instead of Standard Edition.

Most Hardware Load Balancers offer at least layer 4 switching. Such Load Balancers inspect each packet's IP headers and route it to one of the IMS Server farm members based on some rule (e.g., client IP address, destination port, etc.). Most Load Balancers allow continuous monitoring of server status based on custom scripts (e.g., pinging a certain URL).

Some more advanced Hardware Load Balancers may offer layer 7 switching, which can determine which IMS Server farm member to route a packet to based on cookies and URLs. For the purpose of load-balancing IMS Servers, layer 4 switching is good enough.

In a Microsoft NLB setup, all member servers share the same DNS name and virtual IP address. Each server has its own private IP address, for heartbeat checks and administration purposes. Incoming traffic is routed to all servers but only one server will accept the request. All requests from a particular client can be routed to the same server. Members monitor each other's health via heartbeat checks, and re-synchronize among themselves whenever a member goes down or rejoins the cluster.



NLB monitors only the server OS health. If server OS is up but IMS service is down or hung, some IMS Server requests will continue to be routed there.

For more information on IMS clustering, see [Managing IMS clusters](#).

Managing IMS clusters

Refer to this section for details on the deployment of IMS Server in a load balanced two-tier model, with the first tier comprising of the IMS cluster, and the second of a database cluster. The section also details out a path of migration of a deployment from a non-load balanced two-tier configuration to an IMS cluster (load balanced configuration).

This section contains an overview of the IMS load balancing architecture, followed by a brief introduction to the Microsoft Network Load Balancing technology, on which the IMS load balancing architecture is based.

The next topic deals with the steps to be executed for a successful load balanced IMS cluster deployment. It then deals with the migration from an IMS hosted on a single host, to a Microsoft Network Load Balanced (NLB) IMS cluster.

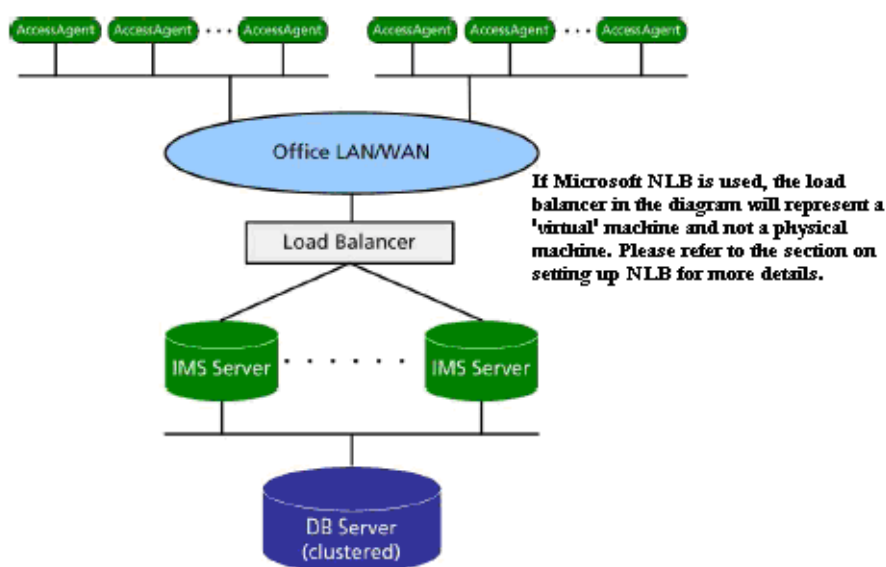


Microsoft NLB is recommended only for small-scale IMS deployments (consisting of not more than two IMS Servers) and for load balancing trials. For large-scale deployments with three or more IMS Servers, hardware load balancers such as the ones offered by vendors such as F5, Cisco, Nortel, Netscaler, etc. should be considered.

Refer to the [Troubleshooting](#) portion of this guide for more information on common issues encountered with using Microsoft NLB.

IMS load balancing architecture

The diagram represents a typical load balanced IMS Server deployment in a large organization. All requests made by the AccessAgent are routed by the load balancer to a particular IMS Server, depending upon the load distribution and other variables. The network load balancer is required to maintain session affinity for a client, or routes all requests within a session for a client, to the same IMS Server. At this point, the concept of distributed requests within the same session is not supported by IMS Server.



IMS Load Balancing Architecture

The communication between the AccessAgent and the IMS is over SSL, indicating the necessity of valid SSL certificates maintained by every IMS Server within the load balanced configuration. Hence, in a load balanced configuration:

- All the individual IMS Servers should have the same SSL certificate, with the identical private keys corresponding to the certificates contained in the key stores.

- All the individual IMS Servers should have the SSL certificates registered to the same virtual host name, since the validity of a SSL certificate necessitates the hostname on the certificate matching the hostname of the 'server' being accessed.



This section discusses the Scalability and High Availability (HA) configuration for IMS Server only, and details pertaining to the HA setup for the database through various clustering technologies is outside the scope of this document.

About the Microsoft Network Load Balancer (NLB)

Operating System families, such as Windows 2000 Server (Advanced Edition only) and Windows 2003 Server, come bundled with a clustering technology, known as Microsoft Network Load Balancing.

This technology provides load balancing of the network traffic across a number of hosts, helping to enhance the scalability and availability of mission critical, IP-based services, including web, Virtual Private Networking (VPN), and others. In other words, NLB dynamically distribute the incoming TCP and UDP traffic among the cluster nodes.

NLB will route requests to member servers of a load-balanced web cluster, provided that the servers are running. If the IMS (or underlying Tomcat) on one of the member servers hangs, crashes, or is brought down, some requests will continue to be routed to this server. A future enhancement is to put in place IMS monitoring scripts for detecting IMS non-responsiveness, and removing the server from the load-balanced cluster, while alerting the IMS Administrator.

For more information on Microsoft Network Load Balancing component, go to this URL: <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/6ac4a6ba-1c0c-46be-8c6a-2c2e0e567e98.mspx>.

Setting up IMS clusters using Microsoft NLB

This topic discusses how to set up an IMS cluster using two scenarios:

- The deployment already has an IMS Server hosted on a single machine. In this case, the issue at hand is the migration of an IMS Server hosted on a single machine, to a load balanced IMS Server configuration. The steps involved in this scenario have been described in [Setting up clusters for existing deployments](#).
- The deployment is a fresh one (e.g., there are no IMS Servers currently installed anywhere). In this instance, we have to figure out a way of deploying a load balanced IMS Server cluster. The setup in this case is detailed out in [Setting up clusters for new deployments](#).

Checklists and assumptions

Checklist before starting:

- For every cluster node, depending upon the number of NIC on the host, assign static IP addresses along with the appropriate hostnames.
- Assign another static IP which shall serve as the virtual IP of the cluster. This should now correspond to the cluster hostname, such as, the hostname with which all the clients will refer to the IMS cluster.
- In the Domain Name Service Tables found on the domain controller, update the hostname to IP address mappings for all the cluster hosts, and add a new entry mapping the virtual hostname to the new IP assigned to it.

For example, assume that the cluster consists of the following machines:

Hostname	IP
imshost1.encentuate.com	10.1.20.1
imshost2.encentuate.com	10.1.20.2
imshost3.encentuate.com	10.1.20.3

Assume also that the cluster hostname and configuration is:

Hostname	IP
ims.encentuate.com	10.1.20.100

The entries will be configured in the DNS tables.

It is assumed that all the machines participating in the NLB cluster have either Windows 2000 Advanced Server or Windows 2003 Server Operating Systems, with the Microsoft Network Load Balancing component installed on them.

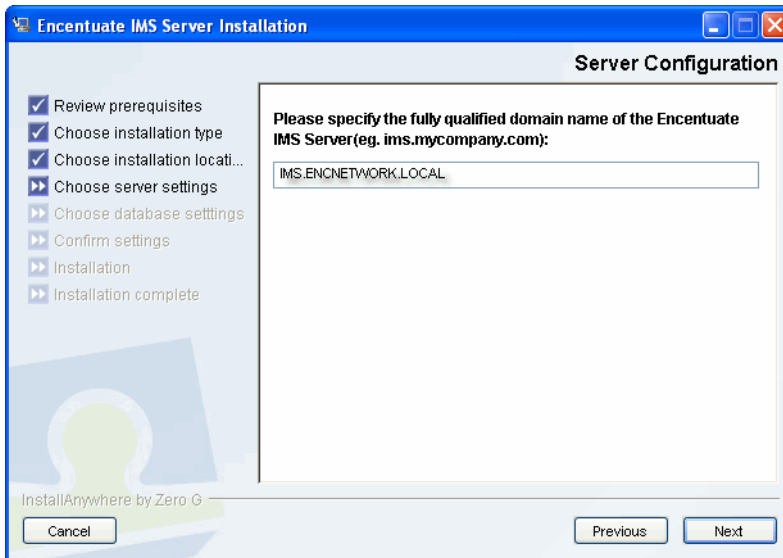
Setting up clusters for new deployments

For a fresh deployment, install IMS Server on one of the hosts, with the hostname of the cluster and NOT the hostname of the actual machine.

For example, if the IMS cluster is going to be referred to by **ims.encentuate.com** install IMS Server on the first machine, **imshost1.encentuate.com** using the hostname **ims.encentuate.com**, as shown in the next graphic.

After installing on one machine, copy the entire IMS Server installation folder to the identical location on the other host machines.

For example, if IMS Server has been installed on **imshost1.encentuate.com** at **C:\Encentuate\IMSServer2.3.0.3**, copy this installation folder to the identical paths on the two other machines, **imshost2.encentuate.com** and **imshost3.encentuate.com**.



Specifying domain name during IMS Server installation

Since copying the installation will also overwrite the IMS configuration file **ims.xml**, which might have been customized to fit the original host's requirements, the configuration changes must be re-entered manually to fit the individual host's requirements. For more information on this discrepancy, see [Upgrading each IMS Server](#).

If fingerprint authentication is used for the deployment, the relevant biometrics software (DigitalPersona and/or UPEK) must be separately installed on each host.

After this setup, it is essential to register the IMSServices, so that they can be configured to start IMS Server on startup on all the machines. To do this, run the batch file **installService.bat** found in the folder **<IMS Installation>\bin\installer** in all machines.

After completing these tasks, you should have all the cluster hosts with identical IMS Server installation folders at the same locations. Based on the checklist in [Checklists and assumptions](#), there should also be a cluster hostname (virtual) and a cluster IP.

Setting up clusters for existing deployments

If the deployment already has an existing IMS Server, the cluster hostname assumes that name of the host machine on which the existing IMS Server is running.

For example if the existing IMS Server is on the machine **ims.encentuate.com**, then our new cluster hostname would have to be **ims.encentuate.com**.

To free up the cluster hostname, rename the host on the original IMS Server. For example, if **ims.encentuate.com** is the cluster hostname, the existing machine **ims.encentuate.com** must be renamed to, for instance, **imshost1.encentuate.com**.

At the end of this step, there are three (3) physical machines: **imshost1.encentuate.com**, **imshost2.encentuate.com**, **imshost3.encentuate.com**, and one (1) virtual hostname **ims.encentuate.com**.

Copy the entire IMS installation directory on the existing IMS Server host (now renamed to **imshost1.encentuate.com** in our examples), to the other hosts, which will be part of the NLB cluster. Note that the paths of all IMS Server installations on all the host machines should be identical, and should also be the same as the path of the original installation.

For example, let us assume the existing IMS Server is hosted on **ims.encentuate.com** (now renamed to **imshost1.encentuate.com**) at **C:\Encentuate\IMSServer3.6.0.0**. Copy the entire **C:\Encentuate\IMSServer3.6.0.0** to the same path in the two (2) other hosts, **imshost2.encentuate.com**, and **imshost3.encentuate.com**.

Copying the installation will also overwrite the IMS configuration file **ims.xml**, which might have been customized to fit the original host's requirements. The configuration changes must be re-entered to fit the individual host's requirements. For more information on this discrepancy, see [Upgrading each IMS Server](#).

If fingerprint authentication is used for the deployment, the relevant biometrics software (DigitalPersona and/or UPEK) must be installed separately on each host.

After this setup, it is essential to register the IMSServices, so that they can be configured to start IMS Server on startup on all the machines. To do this, run the batch file **installService.bat** found in the folder **<IMS Installation>\bin\installer** in all machines.

After completing these tasks, you should have all the cluster hosts with identical IMS Server installation folders at the same locations. Based on the checklist in [Checklists and assumptions](#), there should also be a cluster hostname (virtual) and a cluster IP.

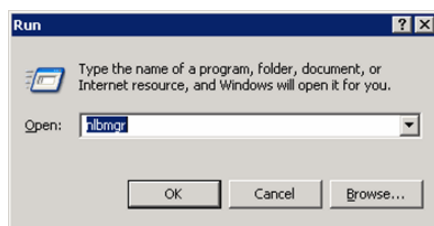
Creating IMS clusters

Select one of the hosts to facilitate the configuration of the NLB using the Network Load Balancing Manager (NLB Manager). The NLB manager is a software component bundled with the Windows Server 2000 and 2003 families, specifically meant to configure and manage a Network Load Balanced configuration.

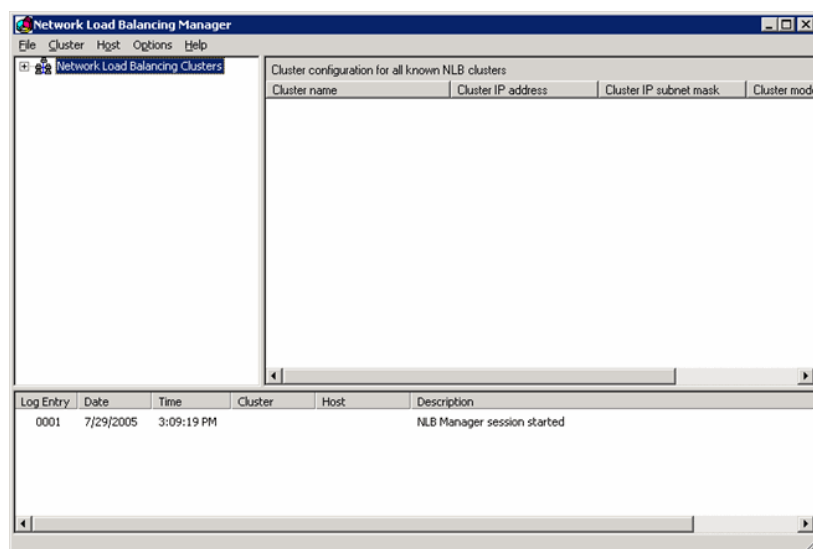
The procedure explains how to make an NLB configuration using the NLB manager on **imshost1.encentuate.com**.

To create an IMS cluster:

- 1 Open the NLB Manager. The Network Load Balancing Manager NLB manager is displayed.
(Start >> All Programs >> Administrative Tools->Network Load Balancing Manager)
(Start >> Run >> type nlbmgr)

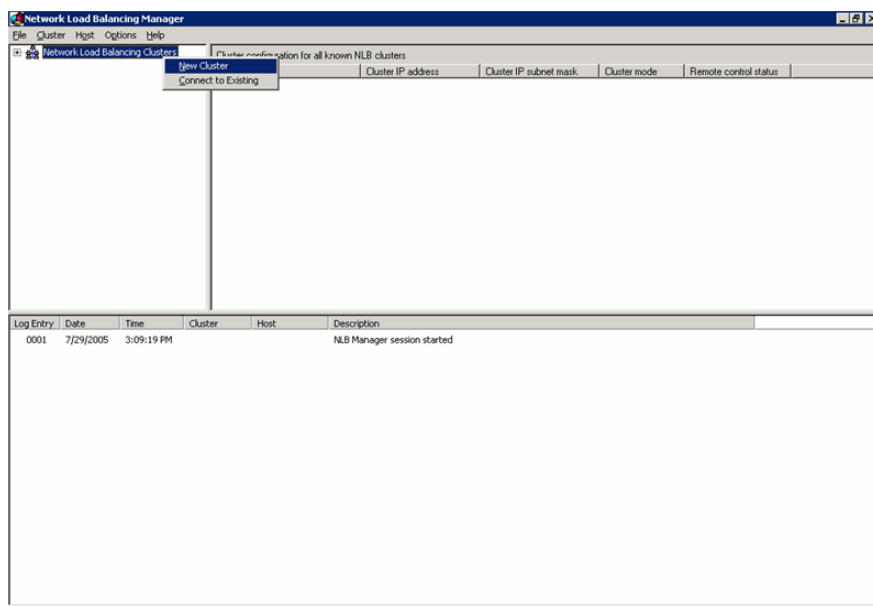


Running NLB Manager



NLB Manager

- 2 Right-click on the **Network Load Balancing Clusters** tree node and select **New Cluster**.



New cluster

The Clusters Parameters window is displayed. For the specific example, the cluster IP address is set at **10.1.20.200**, and the cluster host name is **ims.encentuate.com**.

Cluster Parameters

Cluster IP configuration

IP address: 10 . 1 . 20 . 100

Subnet mask: 255 . 255 . 255 . 0

Full Internet name: ims.encentuate.com

Network address: 03-bf-0a-01-14-64

Cluster operation mode

☐ Unicast ☒ Multicast ☐ IGMP multicast

☐ Allow remote control

Remote password:

Confirm password:

< Back Next > Cancel Help

Cluster Parameters window

- 3 Click **Next** to view the Cluster IP Addresses. Since there are no alternate backup cluster IP addresses, click **Next** again without entering any information in the window.

Cluster IP Addresses

Primary cluster IP address

IP address: 10 . 1 . 20 . 200

Subnet mask: 255 . 255 . 255 . 0

Additional cluster IP addresses

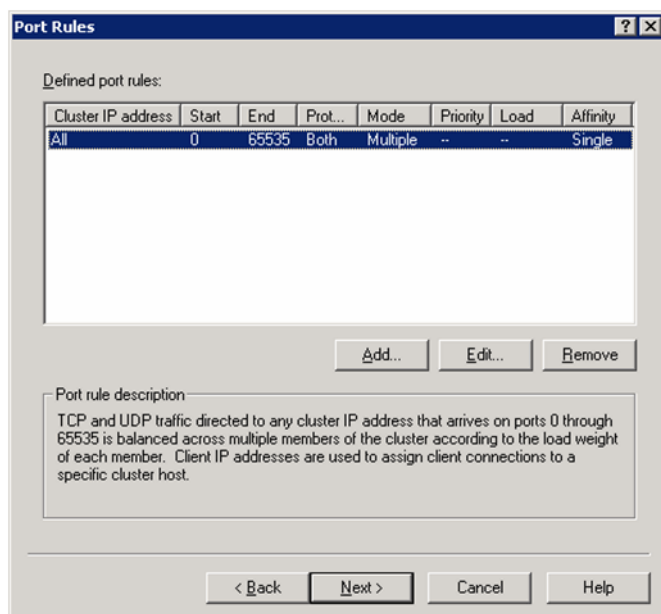
IP address	Subnet mask
------------	-------------

Add... Edit... Remove

Next > Cancel Help

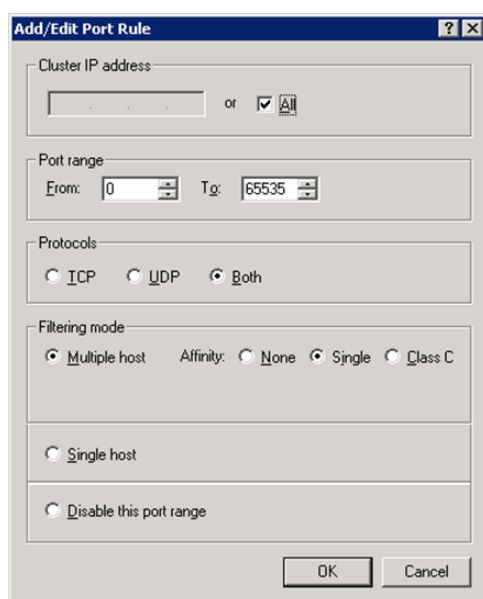
Cluster IP Addresses window

- 5 The next window allows users to set the port rules for the cluster. Since the cluster hosts will be used as dedicated IMS Servers, which make use of ports 443 and 80, there is no need to configure any special port rules. The same port rules are used for all the ports if the default configuration is used.



Port Rules window

To view the actual port rules configuration, click **Edit**. If you need to set up port rules for the IMS only, refer to the listing of the ports, and a sample configuration explained further in this same point.



Add/Edit Port Rule window

A Port Range specifies the range for which these port rules are applicable. A value of **0** to **65535** indicates all the ports of the machines.

Refer to this listing of ports used by IMS Server and its various components:

- **80** - This is the default http port used by IMS Server.
- **443** - This is the default SSL port used for secure communication between the IMS and the AccessAgent.
- **1812** - This is the default port used for Radius authentication. (Older versions of VPN Servers use the UDP port 1645 for this, and it is often not possible for these VPN servers to make their authentication requests at a port different from 1645 on the IMS.)
- **1813** - This is the default port used for Radius accounting. (Older versions of VPN Servers use the UDP port 1645 for this, and it is often not possible for these VPN servers to make their accounting requests at a port different from 1645 on the IMS.)

Refer to the port rules configured for port 80. A similar approach can be taken for all the other listed ports. The summary at the end of this section details the configuration for all the ports.

The screenshot shows the 'Add/Edit Port Rule' window. It contains several sections: 'Cluster IP address' with a text input and an 'All' checkbox; 'Port range' with 'From' and 'To' spinners set to 80; 'Protocols' with radio buttons for TCP, UDP, and Both (selected); and 'Filtering mode' with radio buttons for Multiple host (selected), Single host, and Disable this port range. There are also 'Affinity' radio buttons for None, Single (selected), and Class C. The window has 'OK' and 'Cancel' buttons at the bottom right.

Add/Edit Port Rule window

Protocols

Specifies the protocols for which the rules will apply. Since we operate primarily over TCP, using both should be sufficient.

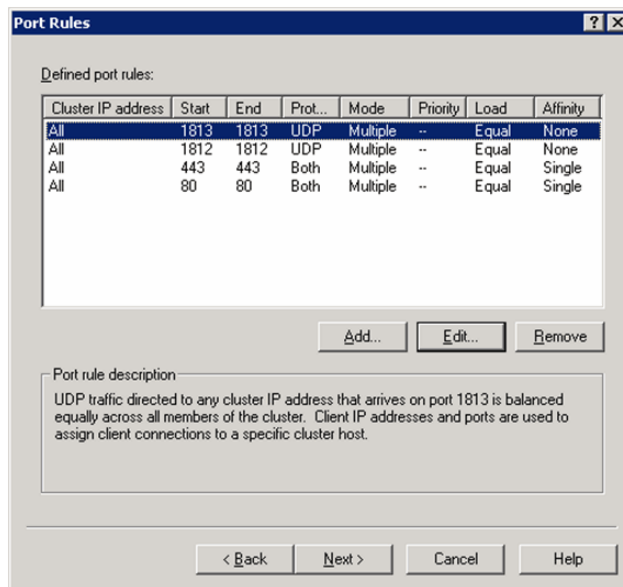
Filtering Mode

Multiple hosts indicate that the load will be balanced over multiple hosts. A single host would configure this setup for a FAILOVER configuration, so that the NLB will ordinarily channel all requests to a single host, and will redirect the requests to the next host only in the event of a failure of the primary host.

Affinity (if the filtering mode is Multiple Host)

When a single affinity is selected, the mapping algorithm uses the clients full IP address. Do not select 'none', since we require client affinity for load balancing IMS Servers.

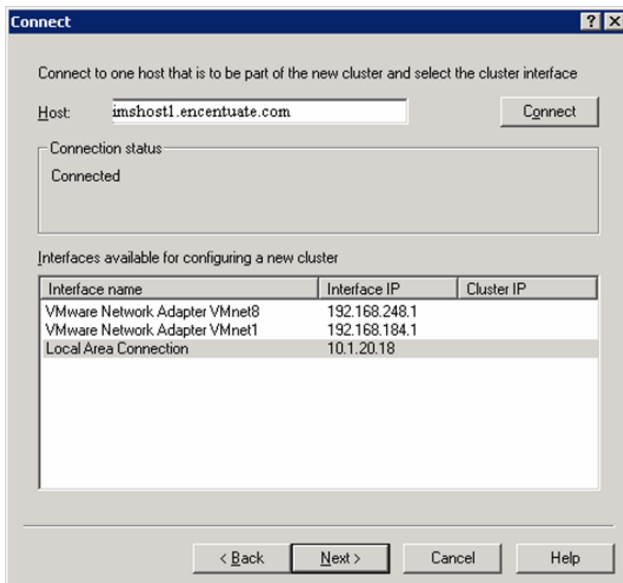
- 6 This is how the port rules window should look like after the configuration is done.



Port Rules window

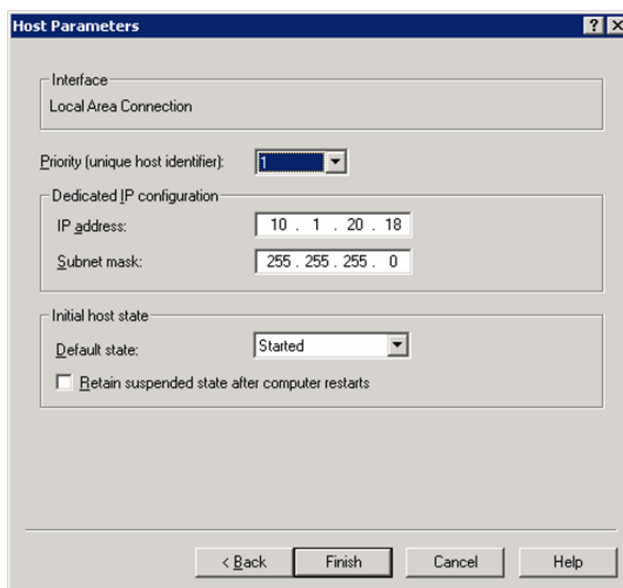
To add hosts to an IMS cluster, click **Next** to start adding nodes.

- 7 Enter **imshost1.encentuate.com** and click **Connect** to add the host to the cluster.



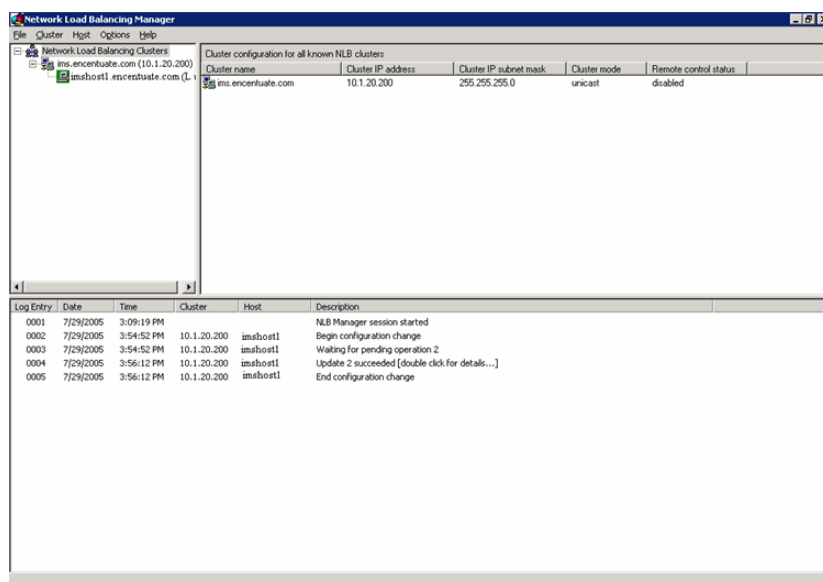
Connect window

- 8 Choose the **Local Area Connection** (the network interface card to be used for the NLB) and click **Next**. The Host parameters configuration will be displayed.



Host Parameters window

- 9 Set the **Priority** of the host, the **IP address**, **Subnet mask**, and **Default State**. In a multiple host configuration, the host priority does not come into effect at all.
- 10 Click **Finish** to add the host to the cluster. After finishing, the Network Load Balance Manager should now display the status of the host as **CONVERGED**, (with the host icon background color set to green). The NLB configuration can now be considered successful. The other hosts can be configured similarly, with decreasing priorities.



Network Load Balancing Manager window (completed configuration)

Maintaining IMS clusters

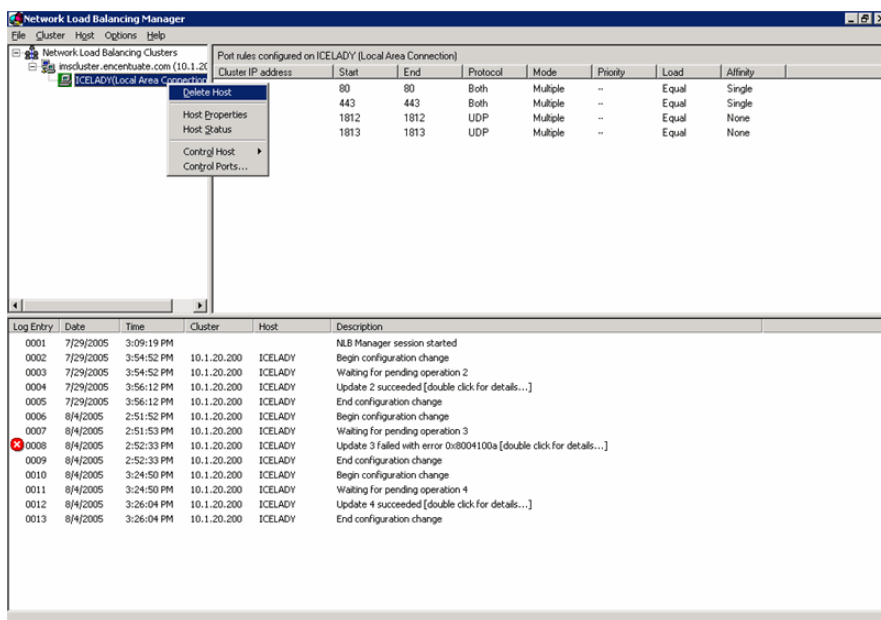
Disassembling IMS clusters

Disassembling the IMS cluster involves removing a cluster from the host and stopping IMS Server on it, over all the hosts. In other words, it is advisable to remove a host from the cluster, and then stop IMS Server running on it, in that sequence.

Once one of the IMS Servers have been removed from the cluster using the NLB manager (see [Creating IMS clusters](#) for details on opening the NLB manager user interface), stop the IMS Server on it. Similarly, for all BUT ONE host in the cluster, remove it first from the node, and only then stop the IMS Server on it. This sequence of actions will reduce the server downtime considerably.

To disassemble an IMS cluster:

- ❶ Open the NLB Manager.
- ❷ To delete the host from the cluster, right-click on the host, and select **Delete Host**.



Network Load Balancing Manager window (Delete Host)

- ③ Delete the last host, the only one remaining in the cluster. Deleting this host will also delete the cluster. The cluster will have to be re-configured, following the steps mentioned in [Creating IMS clusters](#). Stop the IMS Server on this last host.
- ④ Before proceeding any further, back up the IMS configuration file **ims.xml** found in the **installation directory/ims/config**, on all the cluster hosts to a folder outside the standard IMS installation folder. This file contains configurations used by IMS Server running on the specific machine.

Upgrading each IMS Server

Once the cluster has been disassembled, the deployment will no longer have IMS connectivity, and the cluster no longer exists.

To begin the upgrade, choose one of the cluster hosts and perform a standard IMS upgrade. For example, to upgrade the cluster **ims.encentuate.com**, the host **imshost1.encentuate.com** is chosen for upgrade using the IMS installer.

After upgrading the IMS Server, start the IMS Server on the first host. To confirm the successful startup of IMS, access the URL of the IMS Admin User Interface on that host.

Adding the IMS Server back to the cluster

Since the cluster has been disassembled, re-assemble the cluster as needed. The cluster will have to be re-configured from scratch, following the steps mentioned in [Creating IMS clusters](#).

Once the cluster has been re-created using the NLB manager, add the newly upgraded host to the cluster again, using the same configuration as before.

After adding the host to the cluster, test the upgrade, and confirm that the upgrade meets the necessary requirements.

Copying an upgrade to the other hosts

Once the upgrade is functional, copy over the entire installation directory of the upgraded IMS Server to the second host.

The configuration must be done manually, since copying over the installation will replace the IMS configuration file **ims.xml**. The file **ims.xml** might have been customized to fit the host's requirements. Note that just replacing the copied configuration file with the older backed-up configuration file might nullify any changes made by the upgrade.

After making the changes, start the IMS Server on the second host, and verify the successful startup by accessing the IMS Server user interface using the hostname of that machine.

For example, if the host just upgraded is **imshost2.encentuate.com**, the URL used is **http://imshost2.encentuate.com**

After the IMS Server has started up successfully, add the second host to the cluster following steps mentioned in [Creating IMS clusters](#).

Verify that the upgrade is successful using a client whose request is serviced by the second host added to the cluster (**imshost2.encentuate.com**).

Reassembling the cluster

After going through steps in [Copying an upgrade to the other hosts](#) for all the cluster hosts, and verifying that the upgrade is successful, the cluster should have all the original hosts upgraded and functions as before.

Using AccessAdmin

The IMS Server has an interface called AccessAdmin, which is consistent with the interface of AccessAgent. Different access rights are given to the Administrator and Helpdesk roles.

Logging on to AccessAdmin requires certificate authentication. The user must be logged on to a cached Wallet that has either an Administrator or a Helpdesk role. Certain configurations (e.g., system policies and machine policies) can only be viewed but not modified by a Helpdesk user. Like the AccessAgent interface,

AccessAdmin has a left navigation panel for accessing various functions, such as:

- User search and administration (to modify user policies, issue authorization code, unlock a locked Wallet, revoke user, etc.)
- Machine search and maintaining machine policy templates
- Creating and maintaining policy templates (can only be created and maintained by the Administrator, but Helpdesk can view and apply)
- Setting system and application policies (can only be modified by the Administrator, but Helpdesk can view)
- Accessing logs and status information

From the IMS Server machine, you can log on to AccessAdmin by providing a user name and password, without installing AccessAgent.

If required, use the IMS Configuration Utility (*Advanced Settings >> AccessAdmin >> Login >> Allow form-based login to AccessAdmin from remote machine*) to allow user name and password login from any machine.

Encentuate AccessAdmin supports dynamic non-hierarchical groups, collapsible sections, and the setting of policies for groups and users. Attributes that define logical groups (e.g., department) can be obtained directly from the corporate directory.

When the user signs up or a machine joins the IMS Server, policies are initially assigned based on the machine's/user's attributes that match the policy template.

Subsequently, user groups are dynamic because membership depends on the user's policies. For example, a user may belong to the group of RFID users because the authentication policy is "Password + RFID". By changing the authentication policy for the user to "USB Key", the user becomes a member of the group of USB Key users.

User policy modifications can be performed on individual users or on entire groups of users. A user may belong to the group of all USB Key users, as well as the group of all AccessAssistant users. Since groups are based on search criteria, they are virtual and they overlap.

User policy templates can be defined for specific groups of users to facilitate policy setting. For example, a template can be defined for the Finance department. Any new user whose department attribute is "Finance" will have the policies initialized with the template settings.

Machine policy templates are defined for each machine that joins the IMS Server. These policies are under scope:machine (scp_machine), and keyed on the machine name. The machine policies are synced through incremental synchronization based on the machine name.

Machines can be assigned to an existing machine policy template based on either or all of the following attributes:

- Machine name
- IP address
- AccessAgent version
- OU group
- Active Directory security group

All policies with system, machine or user scope can be modified through AccessAdmin. User policies can also be modified for an entire group of users by using the "Search Users" feature. System policies may be defined for authentication services, applications, or a combination of authentication service and application.

The Helpdesk role can be defined for different groups of users. A user taking on the Helpdesk role associated with a group can manage (e.g., authorize and revoke) users only for that group. Helpdesks may manage overlapping groups of users.

AccessAdmin is also used to issue authorization codes to users. Each authorization code has a selectable life span.

Role assignment features

By default, all new users are assigned User roles. To reassign roles to either Helpdesk or Administrator, it would have to be done using either AccessAdmin or the IMS Configuration Utility, depending on the number of users to be reassigned at that certain time.

To reassign one user at a time, usually from a User role to a Helpdesk role, use AccessAdmin and refer to [Reassigning roles for Helpdesk users](#). To reassign several users at a time, use the IMS Configuration Utility and refer to [Automatic role assignment for large deployments](#).

Reassigning roles for Helpdesk users

Use AccessAdmin to change the role of the user. By default, when users sign up, all users are automatically assigned the role User, except for those who have been pre-defined as Administrators during IMS Server installation. Administrators are automatically assigned the Administrator role during sign-up.

Using AccessAdmin, a user can be assigned to a Helpdesk role manually. However, it becomes tedious if the Administrator must reassign hundreds of users. Therefore, an automatic role assignment feature must be provided.

Currently, you can assign one or more existing Helpdesk persons to a policy template. However, the problem arises when a new Helpdesk user signs up, and this new person would need to be added to the template manually.

If each new Helpdesk user is allowed to manage all users, enable the feature for automatic assignment of all policy templates and users to the new Helpdesk user (*AccessAdmin >> User Attributes >> Automatic assignment of all policy templates and users to new Helpdesk user*).

Automatic role assignment for large deployments

For larger deployments, there may be a large number of Helpdesk users and Administrators, and it may be too tedious to manually assign roles to them through AccessAdmin. There may be an Active Directory attribute that is used to distinguish between Users, Helpdesks, and Administrators.

The automatic role assignment feature in Encentuate IAM Enterprise allows users to assign the appropriate roles (e.g., User, Helpdesk, Administrator) automatically during sign-up, based on a particular Active Directory attribute.

To enable the feature, use the IMS Configuration Utility to configure the following settings:

- ❶ Ensure that the automatic role assignment bind task is in the bind task list (*IMS Server >> Miscellaneous >> Application Binding Tasks*).
- ❷ Specify the Active Directory attribute for automatic role assignment (*AccessAdmin >> User Attributes >> Role assignment attribute*).



The usual Active Directory attributes that may be used are "memberOf", "title", "description", and "department". The Active Directory attribute for role assignment can be multi-valued (e.g., memberOf). For multi-valued Active Directory attributes, all the values will be taken into consideration. It will be treated as a match provided that one of the values matches what is configured for the role assignment.

- ❸ Define the mapping between Active Directory attribute values and roles (*AccessAdmin >> User Attributes >> Role assignment mapping*).



Users in the list of pre-defined Administrators (defined during IMS Server installation) will be assigned the Administrator role regardless of their Active Directory attribute value for automatic role assignment.

Take note of the following on the automatic role assignment feature:

- **Automatic role assignment does not apply to existing users.**

Automatic role assignment is only used when a user signs up or is provisioned. It does not apply to existing Encentuate IAM Enterprise users. The roles of existing users will not change when the automatic role assignment configuration is modified, or when a user's Active Directory attribute for role assignment is modified.

- **The Active Directory attribute for role assignment must not be nested.**

Some Active Directory attributes may be nested. For example, the "memberOf" attribute specifies a user's direct Active Directory group membership. However, since groups can be members of other groups, this nested relationship among groups also applies to users.

In the current implementation, the IMS Server will not traverse the nested relationship among groups, and cannot properly handle AD attributes (e.g., "memberOf"). If "memberOf" is used, users must be "direct members" of the groups to be used for role assignment.

- **The automatic assignment of existing policy templates and users to new Helpdesk user is limited to one of the two settings:**

- **Enabled:** This assigns all existing policy templates and users to a new Helpdesk user. The assumption is that each Helpdesk user should be allowed to manage all Encentuate IAM Enterprise users.
- **Disabled:** This will not assign any policy template or user to a new Helpdesk user. The Administrator must manually assign the appropriate policy templates and users to each new Helpdesk user.

Managing remote access for IMS Servers

This section describes the various options of deploying IMS in an enterprise, so remote users can access IMS over the Internet. This is useful for users who are in overseas locations, or even users who use the AccessAdmin at home and do not connect to a VPN.

The assumption is that these remote users connect to IMS, either via their AccessAdmin for IMS services, or via the browser for the AccessAdmin interface.

Setting up IMS proxies on dedicated servers

The IMS Server is located in the internal network, and is not directly accessible from the Internet.

An IMS proxy is placed in the DMZ and is accessible from the Internet. **ims.company.com** on public DNS maps to this proxy. This proxy can be implemented as a simple servlet running on a web server.

This proxy forwards all requests to IMS Server. It can be programmed to do further filtering, such as accept only valid IMS XML messages. The proxy performs one-way SSL with the client.

The IMS DB can be configured to be only physically accessible by the IMS Server.

The pros for this type of setup include the following:

- IMS Server remains in the internal network. The DMZ can be shut down and IMS will still work for internal users.
- Compared to [Setting up IMS proxies on existing web applications](#), this option does not require us to configure the enterprise's existing web server(s).
- Compared to [Port forwarding](#), this can do more intelligent filtering.
- The proxy is vulnerable to DoS attack, though the actual IMS Server is unaffected and can still serve internal users.

The cons for this type of setup include the following:

- Needs to either run on its own machine, which increases cost and administration work.
- Run a separate instance of an existing web server, which requires the company to open new ports on the outside firewall.

This assumes that the existing web server uses standard ports (80 & 443). This also means that users installing AccessAdmin externally know about these ports, which are different from the ones they use when they install internally.

For example, to install AccessAgent internally, users connect to IMS on port 443, which is the default value. But to install AccessAgent externally (e.g., at home), users must manually change the default port to another value.

Setting up IMS proxies on existing web applications

This option is very similar to [Setting up IMS proxies on dedicated servers](#), except that the proxy is set up in an existing web application. This option is recommended when installing an Authentication Bridge on one of the applications in the DMZ, which means just adding another proxying filter.

The pros for this type of setup include the following:

- IMS Server remains in the internal network. The DMZ can be shut down and IMS will still work for internal users.
- Compared to [Port forwarding](#), this can do more intelligent filtering.
- No need for an external firewall to open additional ports; it just rides on an existing web application, which presumably uses standard ports.

The cons for this type of setup include the following:

- This requires configuring an existing web application. For example, we need to detect IMS requests based on URL pattern and proxy them to the backend IMS.
- The proxy is vulnerable to DoS attack, though the actual IMS Server is unaffected and can still serve internal users.

Port forwarding

Configure the external router so that all requests to a port are forwarded to the backend IMS Server automatically. Port forwarding is an operation that blindly forwards all received packets from a particular port to another server/port.

For example, you can configure the router to do the following:

```
TCP/IP on Port 80 ---forward to---> Port 8080 on 10.1.16.18
```

```
TCP/IP on Port 25 ---forward to---> Port 25 on 10.1.16.6
```

Map **ims.company.com** on public DNS maps to this router.

The IMS can either get its own dedicated router (e.g., **ims.encentuate.com**), or it can use an existing router for other servers, in which case it will need additional ports if 80 and 443 are already taken.

The pros for this type of setup include the following:

- The IMS Server remains in the internal network. The DMZ can be shut down and IMS will still work for internal users.
- It is easy to implement (if allowed).

- There will be no need for additional IMS proxy.

The cons for this type of setup include the following:

- It requires the company to set aside new ports for external IMS access, if the IMS shares a router (where 80 and 443 are already taken). This will then require opening new firewall ports. Users must know these ports, which are usually different from the ones they use internally.
- Compared to [Setting up IMS proxies on dedicated servers](#) and [Setting up IMS proxies on existing web applications](#), this can do only very primitive forwarding. Further filtering based on request content is not possible.

Placing IMS in DMZ

This option places IMS Server in the DMZ, out of the internal network.

The pros for this type of setup include the following:

- There will be no need for a separate IMS Proxy.
- There will be no need for additional ports.
- It is simple to implement.

The cons for this type of setup include the following:

- There is no clean separation of DMZ and the internal network. Internal users have to connect to IMS out of the DMZ. Internal users cannot use IMS when the DMZ is shut down.
- IMS is more vulnerable to external attacks, such as DoS.

Provisioning Setup

This chapter covers the following topics:

- [Provisioning API](#)
- [About Encentuate Provisioning Agent](#)

Provisioning API

Provisioning systems have increasingly become critical components of the enterprise identity and access management strategy. A provisioning system provides identity lifecycle management for application users in enterprises and manages their credentials.

Encentuate IAM Enterprise, an enterprise access security solution, provides real-time implementation of access security policies for users and applications.

An integration between a third-party identity provisioning system with Encentuate IAM enterprise access security solution results in the following:

- A complete identity and access management solution that provides automatic application account provisioning
- A central view of all application accounts
- Sign-on/sign-off automation
- Authentication management
- User-centric audit logs and report generation
- Centralized de-provisioning for all accounts

The Encentuate IAM Enterprise API for provisioning enables third-party identity provisioning systems to integrate with the IMS Server. The developer can use the Java API or SOAP API.

For more information on Encentuate IAM API, see the IAM Provisioning Integration Guide.



To provision applications accounts into a user's Wallet, the user must log on with a cached Wallet. Provisioning of application accounts fail if `pid_wallet_caching_option` is 0 or if the user chooses not to cache the Wallet.

Provisioning of application accounts can only work for cached Wallets created by AccessAgent version 3.1.5.12 and above. If Wallets were cached by earlier versions of AccessAgent, they need to be deleted and re-cached with AccessAgent version 3.1.5.12 and above.

About Encentuate Provisioning Agent

If an enterprise uses Active Directory as the enterprise directory, it would usually use the Active Directory management console to manage its users. User management activities include setting of user attributes, disabling accounts and de-provisioning accounts.

However, after deploying Encentuate IAM Enterprise, the enterprise would potentially have to manage users from IMS Server's administrative user interface (AccessAdmin), as the IMS Server manages the users' Wallets containing all applications credentials, audit logs, and policies.

When a user needs to be de-provisioned, the Administrator would need to de-provision the user from both the IMS Server and Active Directory. To reduce administrative effort, the Administrator can use the IMS Server as the central administration server. When an IMS user is de-provisioned through AccessAdmin, the IMS Server can delete the user's Active Directory account from Active Directory using a connector.

Some enterprises may not want to change their existing business and Helpdesk processes of de-provisioning users through the Active Directory management console. In such cases, the Encentuate provisioning agent would be used. With the Encentuate provisioning agent, the Administrator or Helpdesk can de-provision users from the Active Directory management console. The Encentuate provisioning agent would then automatically de-provision the corresponding IMS users from the IMS Server.



Although the component is called "provisioning agent", it can only de-provision IMS users when the users have been de-provisioned in Active Directory. If the need arises, other provisioning features may be added in the future.

Solution overview

This section describes the high-level specifications of the Encentuate provisioning Active Directory agent, as well as the various deployment options.

The Encentuate provisioning agent is installed as a separate entity, which uses the IMS provisioning APIs to perform the provisioning and de-provisioning tasks. The agent can be configured such that it checks with Active Directory or ADAM to determine user account status, various user attributes, etc.

No administrative overhead for Active Directory-based user de-provisioning

The solution does not add administrative overhead for user de-provisioning through the Active Directory management console.

No modification to existing Active Directory and provisioning infrastructure

The solution does not require modification to existing Active Directory and provisioning infrastructure. This eliminates the need to obtain approvals for infrastructure modifications, which are usually tedious and may take too long.

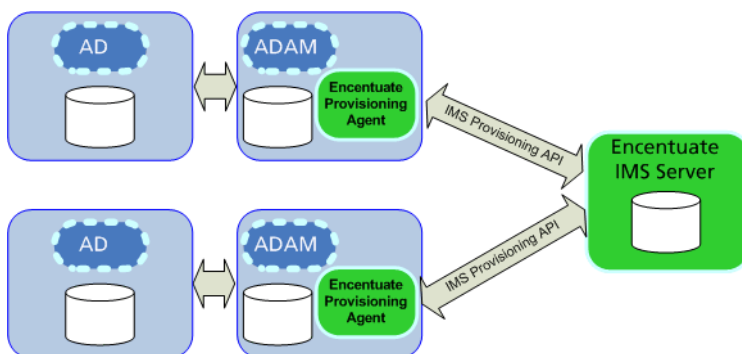
Complete de-provisioning of accounts

When users are de-provisioned on Active Directory, the solution performs a complete de-provisioning of the corresponding IMS users. Depending on customer preference, the IMS users can be either revoked or deleted. This includes the revocation of the users' authentication factors, disabling of users' Wallets, creation of audit logs, etc. It ensures that deprovisioning complies with relevant legislations, such as SOX.

Deployment options

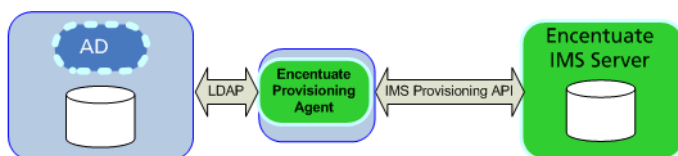
It is recommended that the Encentuate provisioning agent is installed on the same machine as ADAM. In that case, the search functions will be faster as ADAM has its own cached copy of the user directory. However, the Encentuate provisioning agent can also be configured to directly communicate with Active Directory.

An enterprise may have one or multiple ADAMs. If there are multiple ADAMs supporting multiple domains, each ADAM machine would host one Encentuate provisioning agent. The next diagram illustrates such a structure.



Encentuate provisioning agent periodically checks status of accounts in ADAM and accord de-provisions accounts in IMS Server.

The next diagram illustrates how the Encentuate provisioning agent can also be configured to communicate with Active Directory directly:



Encentuate provisioning agent periodically checks status of accounts in Active Directory and accordingly de-provisions accounts in the IMS Server.

General prerequisites

The solution assumes that the enterprise uses Active Directory as the enterprise directory, and that the Active Directory management console is used for user management, to set user attributes, disable accounts, and de-provision accounts.

Workflow and use case

Currently, the product only supports the following use case: De-provisioning IMS user when AD account is de-provisioned.

The Administrator or Helpdesk can de-provision a user from the Active Directory management console as follows:

- In the Active Directory management console, de-provision the user.
- Encentuate provisioning agent detects (through periodic polling) that a user has been de-provisioned on Active Directory.
- Encentuate provisioning agent invokes IMS Server's provisioning API to de-provision the IMS user.

- User's authentication factors are automatically revoked.
- At user's next login attempt through AccessAgent, the user is informed that the account has been revoked.

Installation and configuration

This section contains installation and configuration instructions for the Encentuate provisioning agent. It is assumed that an IMS Server has already been installed and configured.

The Encentuate provisioning agent is distributed as a compressed (ZIP) archive. The archive exists in two different versions. The difference between the versions is whether the Java Runtime Environment (JRE) is included in the distribution. The archives and their sizes are:

- EncentuateProvAgent.zip (34.0 MB)
- EncentuateProvAgent_NoJRE.zip (5.29 MB)

The directory structure of the distributable archive is as follows:

- **bin**: The binary files from which the Encentuate provisioning agent can be started, stopped, and installed/uninstalled as a Windows service.
- **config**: The Encentuate provisioning agent configuration files.
- **docs**: The Encentuate provisioning agent documentation.
- **j2re1.5.0**: The JRE, if it is included in the archive.
- **lib**: The libraries that are needed by the Encentuate provisioning agent.
- **logs**: The location of the log files.

The Encentuate provisioning agent requires JRE version 1.5.0 or above. If this is not provided in the distributable archive, it can be downloaded from <http://www.java.com>. After installing the JRE, the system property JAVA_HOME must be set to the base directory of the JRE installation (e.g., C:\j2re1.5.0).

Installing the Encentuate provisioning agent

To install the Encentuate provisioning agent:

- ① Set up a new **IMS Bridge** using the IMS Configuration Utility (*IMS Bridges >> Configure*) on the IMS Server that will connect to the Encentuate provisioning agent.

Specify the IP address (IMS Bridge IP Addresses) of the machine where the Encentuate provisioning agent will be installed. Create a new user name (Name) and password (IMS Bridge password) for the IMS Bridge. These will be used later in the Encentuate provisioning agent configuration.

- ❷ Unzip the distributable archive to a directory (e.g., **C:\Encentuate**), making sure to maintain the directory structure in the archive.
- ❸ The Encentuate provisioning agent uses one-way SSL to communicate with the IMS Server. This means that the IMS Server's SSL certificate must be trusted by importing it into a trust store. The trust store can either be a pre-existing one used by other applications or the trust store provided in "config\truststore.jks".

To import the Base-64 certificate to a trust store, use the java **keytool.exe** command-line tool. The following is an example usage: **j2re1.5.0\bin\keytool.exe -import -alias lmsSsl -file C:\Encentuate\sslCert.cer -keystore C:\Encentuate\config\truststore.jks**.

Configuring the Encentuate Provisioning Agent

Configure the Encentuate provisioning agent by editing the **agentConfig.xml** file located in the **config** directory. For example, if the archive was unzipped to **C:\Encentuate**, the configuration file will be at **C:\Encentuate\config\agentConfig.xml**.

The configuration keys for the Encentuate provisioning agent are as follows:

■ provisioningagent.ldapAttrs

Description:

The LDAP attributes will be cached by the Encentuate provisioning agent and be used to determine the corresponding user name on IMS Server. This configuration can contain multiple values. It is optional and the default value is sAMAccountName.

Example:

```
<provisioningagent.ldapAttrs>

    <value xml:lang="en">FirstAttribute</value>

    <value xml:lang="en">SecondAttribute</value>

</provisioningagent.ldapAttrs>
```

■ provisioningagent.ldapSearchFilter

Description:

The LDAP search filter that will be used when searching for users. This configuration is optional and by default there is no search filter.

Example:

```
<provisioningagent.ldapSearchFilter>

    <value xml:lang="en">(sAMAccountName=A*)</value>

</provisioningagent.ldapSearchFilter>
```

■ provisioningagent.revokeOrDeleteUser

Description:

Whether a user should be revoked or deleted from the IMS Server when the user is detected as removed from Active Directory. There are two possible values for this configuration key: **revoke** and **delete**. This configuration is optional and. The default value is **revoke**.

Example:

```
<provisioningagent.revokeOrDeleteUser>

    <value xml:lang="en">revoke</value>

</provisioningagent.revokeOrDeleteUser>
```

■ provisioningagent.maxRemovalAttempts

Description:

The number of attempts the Encentuate provisioning agent should make to remove a user from IMS Server. After the maximum number of removal attempts, an error will be logged in the Windows Event Log and no further action will be taken on that user. This configuration value must be an integer. It is optional and the default value is **5**.

Example:

```
<provisioningagent.maxRemovalAttempts>

    <value xml:lang="en">5</value>

</provisioningagent.maxRemovalAttempts>
```

■ provisioningagent.userCacheFile

Description:

The location of the file where the users from Active Directory will be cached. A configuration value is optional and the default value is **userCache.xml** (of the working directory from which the application is launched).

Example:

```
<provisioningagent.userCacheFile>

    <value xml:lang="en">userCache.xml</value>

</provisioningagent.userCacheFile>
```

■ provisioningagent.executionIntervalMinutes

Description:

The interval that the Encentuate provisioning agent will poll Active Directory or ADAM for changes. When a change is detected, the agent will de-provision the user from IMS Server. This configuration must be an integer. It is optional and the default value is **30**.

Example:

```
<provisioningagent.executionIntervalMinutes>

    <value xml:lang="en">30</value>

</provisioningagent.executionIntervalMinutes>
```

■ provisioningbridge.userName

Description:

The user name used to authenticate with the IMS Server. A configuration value is required.

Example:

```
<provisioningbridge.userName>

    <value xml:lang="en">TheUserName</value>

</provisioningbridge.userName>
```

■ provisioningbridge.password

Description:

The password used to authenticate with the IMS Server. A configuration value is required.

Example:

```
<provisioningbridge.password>

    <value xml:lang="en">ThePassword</value>

</provisioningbridge.password>
```


■ **ims.serverName**

Description:

The host name of the IMS Server. Note that the value is not a URL. It should not contain protocol information. A configuration value is required.

Example:

```
<ims.serverName>

    <value xml:lang="en">ims.yourcompany.com</value>

</ims.serverName>
```

■ **ims.httpsPort**

Description:

The port where IMS Server listens for HTTPS requests. This configuration is optional, with the default value of **443**.

Example:

```
<ims.httpsPort>

    <value xml:lang="en">443</value>

</ims.httpsPort>
```

■ **ims.httpPort**

Description:

The port where IMS Server listens for HTTP requests. This configuration is optional, with the default value of **80**.

Example:

```
<ims.httpPort>

    <value xml:lang="en">80</value>

</ims.httpPort>
```

■ **ims.servicePath**

Description:

The root path of IMS Server services. This configuration is optional, with the default value **/ims/services/**. Note that the value should start with **/**.

Example:

```
<ims.servicePath>

    <value xml:lang="en">/ims/services/</value>

</ims.servicePath>
```

■ provisioningbridge.trustStore

Description:

The trust store used by the provisioning bridge. The trust store should contain the SSL certificate of the IMS Server which will be connecting to the bridge. This configuration does not take effect if there is a system property set for `javax.net.ssl.trustStore`.

Example:

```
<provisioningbridge.trustStore>

    <value xml:lang="en">C:\path\to\truststore</value>

</provisioningbridge.trustStore>
```



The full name of `truststore.jks` must be specified in `agentConfig.xml`. Java 1.5 expects the full file path or else it will trigger the following exception: "Unexpected error:java.security.InvalidAlgorithmParameterException: the trustAnchors parameter must also be non-empty".

■ provisioningbridge.trustStorePassword

Description:

Password of the trust store used by the provisioning bridge. This configuration does not take effect if there is already a system property set for `javax.net.ssl.trustStorePassword`.

Example:

```
<provisioningbridge.trustStorePassword>

    <value xml:lang="en">password</value>

</provisioningbridge.trustStorePassword>
```

■ connector.ldap.agent.server_uri

Description:

The LDAP server URI. Location of the Active Directory server (e.g., `ldap://machinename`). A configuration value is required.

Example:

```
<connector.ldap.agent.server_uri>

    <value xml:lang="en">ldap://machinename</value>

</connector.ldap.agent.server_uri>
```



The agent can be configured for connecting via LDAPS which is LDAP over SSL. Just set the **connector.ldap.agent.server_uri** entry to **ldaps://Active DirectoryName:636**.

■ **connector.ldap.agent.lookup_userid**

Description:

The Active Directory user name with permissions for lookup operations. If not set, the Active Directory must support anonymous connections.

Example:

```
<connector.ldap.agent.lookup_userid>

    <value xml:lang="en">TheUserName</value>

</connector.ldap.agent.lookup_userid>
```

■ **connector.ldap.agent.lookup_password**

Description:

The corresponding password for the Active Directory user name with permissions for lookup operations.

Example:

```
<connector.ldap.agent.lookup_password>

    <value xml:lang="en">ThePassword</value>

</connector.ldap.agent.lookup_password>
```

■ **connector.ldap.agent.lookup_user_base_dn**

Description:

The base distinguished name (DN) of the lookup Active Directory user. A configuration value is required.

Example:

```
<connector.ldap.agent.lookup_user_base_dn>

    <value xml:lang="en">CN=Users,DC=company,DC=com</value>

</connector.ldap.agent.lookup_user_base_dn>
```

■ connector.ldap.agent.user_tree_dn

Description:

The distinguished names (DNs) of the users in Active Directory. A configuration value is required.

Example:

```
<connector.ldap.agent.user_tree_dn>

    <value xml:lang="en">CN=Users,DC=company,DC=com</value>

</connector.ldap.agent.user_tree_dn>
```

■ connector.ldap.agent.context_factory

Description:

The fully qualified class name of the factory class that creates an initial context. A configuration value is optional and the default value is **com.sun.jndi.ldap.LdapCtxFactory**.

Example:

```
<connector.ldap.agent.context_factory>

    <value xml:lang="en">com.sun.jndi.ldap.LdapCtxFactory</
value>

</connector.ldap.agent.context_factory>
```

■ connector.ldap.agent.security_protocol

Description:

The protocol used to connect to Active Directory. There are two possible values for this configuration: **ssl** and **none**. A configuration value is optional and the default is **none**.

Example:

```
<connector.ldap.agent.security_protocol>

    <value xml:lang="en">none</value>

</connector.ldap.agent.security_protocol>
```

■ connector.ldap.agent.authentication

Description:

The mechanism used to authenticate with Active Directory. There are two possible values for this configuration: **simple** and **none**. A user name and password are required for **simple** authentication, while an anonymous bind is done when **none** is configured. A configuration value is optional and the default value is **simple**.

Example:

```
<connector.ldap.agent.authentication>

    <value xml:lang="en">simple</value>

</connector.ldap.agent.authentication>
```

■ connector.ldap.agent.referral

Description:

Specifies how referrals returned by the LDAP server are processed. There are two possible values for this configuration: **follow** and **ignore**. If set to **follow**, any referrals will be followed automatically. If set to **ignore**, any referrals will be ignored. A configuration value is optional and the default value is **follow**.

Example:

```
<connector.ldap.agent.referral>

    <value xml:lang="en">follow</value>

</connector.ldap.agent.referral>
```

■ connector.ldap.agent.search_scope

Description:

Specifies the scope for user search on the LDAP server. There are two possible values for this configuration: **one_level** and **sub_tree**. If set to **one_level**, a single level is searched for users. If set to **sub_tree**, the entire sub-tree is searched for users. A configuration value is optional and the default value is **one_level**.

Example:

```
<connector.ldap.agent.search_scope>

    <value xml:lang="en">one_level</value>

</connector.ldap.agent.search_scope>
```

■ `connector.ldap.agent.user_dn_attribute`

Description:

The distinguished name (DN) attribute for the users. A configuration value is optional and the default is **cn**.

Example:

```
<connector.ldap.agent.user_dn_attribute>

    <value xml:lang="en">cn</value>

</connector.ldap.agent.user_dn_attribute>
```

■ `connector.ldap.agent.count_limit`

Description:

The maximum number of user names retrieved from Active Directory when searching for users. The value should be greater than the page size. A configuration value is optional and the default value is **200**.

Example:

```
<connector.ldap.agent.count_limit>

    <value xml:lang="en">200</value>

</connector.ldap.agent.count_limit>
```

■ `connector.ldap.agent.time_limit`

Description:

The maximum time (in milliseconds) before a connection time-out occurs. A configuration value is optional and the default value is **3000**.

Example:

```
<connector.ldap.agent.time_limit>

    <value xml:lang="en">3000</value>

</connector.ldap.agent.time_limit>
```

■ `connector.ldap.agent.page_size`

Description:

The user names retrieved from Active Directory are retrieved in groups (called pages) to obtain all the users without exceeding the maximum retrieval limit. This value is the size of that page, which must be less than the maximum retrieval limit. A configuration value is optional and the default value is **100**.

Example:

```
<connector.ldap.agent.page_size>  
  
    <value xml:lang="en">100</value>  
  
</connector.ldap.agent.page_size>
```

Starting the Encentuate provisioning agent

Before starting the Encentuate provisioning agent, test the configurations by launching the Encentuate provisioning agent from the command-line with the console option as follows:

```
C:\Encentuate\bin\enPrvAgt.bat console
```

The Encentuate provisioning agent will query Active Directory or ADAM. Verify the connection based on the displayed log messages. If there are errors, the configuration values must be corrected. Use **Ctrl+C** to stop the Encentuate provisioning agent and check the configuration settings before trying again.

To install the Encentuate provisioning agent as a Windows service, launch the Encentuate provisioning agent from the command-line with the install option as follows:

```
C:\Encentuate\bin\enPrvAgt.bat install
```

The Encentuate provisioning agent will then be started automatically whenever the computer starts up.

You can also manually start the Encentuate provisioning agent service with the following command:

```
C:\Encentuate\bin\enPrvAgt.bat start
```

Configuring Encentuate provisioning agent (Advanced)

By default, the Encentuate provisioning agent uses the Active Directory user's sAMAccountName as the IMS user's Encentuate user name (Enterprise Login). If desired, another Active Directory attribute may be used as the IMS user's user name.

To configure using the IMS Configuration Utility:

- ❶ In the IMS Configuration Utility, go to *IMS Server >> IMS and LDAP User Association*.

`encentuate.ims.service.uadmin.SingleAttributeMatcher` should be included in the Matchers Classes.

- ❷ Set the **LDAP Attribute Name** to the desired Active Directory attribute (e.g., `displayName`) to be used as the Encentuate user name.
- ❸ Set the **IMS Attribute Name** to **Enterprise Login**.



If LDAP Attribute Name is set to "displayName", the IMS user will not be de-provisioned if the displayName contains a space (e.g., "Firstname Lastname"). The IMS user name cannot contain spaces.

ADAM configuration

If ADAM is used, configure Active Directory synchronization as follows for the Encentuate provisioning agent to work:

- The user's **sAMAccountName** should be synchronized from Active Directory to ADAM.
- The user's **X.500 DN** on ADAM (e.g., `CN=john,OU=us,DC=encentuate,DC=com,DC=adam`) may not be the same as his **X.500 DN** on Active Directory (e.g., `CN=john,OU=us,DC=encentuate,DC=com`). ADAM and MIIS/ADAM synchronization need to be correctly configured to ensure that their DNs are the same.

Policy settings

No policy settings are needed for the Encentuate provisioning agent.

Issues and notes

Take note of the following on Encentuate provisioning agent:

De-provisioning a user on Active Directory does not de-provision the IMS user immediately

The Encentuate provisioning agent polls Active Directory or ADAM periodically for recently de-provisioned users and performs the de-provisioning actions on the IMS Server accordingly. This implies that the de-provisioning of IMS users may not happen immediately after an Active Directory user is de-provisioned.

To notify the Encentuate provisioning agent immediately when a user is de-provisioned on Active Directory implies that some agent has to be deployed onto Active Directory itself. This means Active Directory has been modified, which goes against the original specification of no modification to infrastructure.

Even if ADAM is used, the MIIS/IIFP synchronization process is not event-driven. The MIIS Administrator needs to set up periodic scripts to synchronize Active Directory into MIIS, and periodic scripts to synchronize MIIS to ADAM. The frequency of synchronizing Active Directory changes to ADAM depends on how frequently the synchronization scripts are run.

Provisioning a user on Active Directory does not provision the IMS user immediately

The Encentuate provisioning agent does not automatically provision IMS users when users are provisioned on Active Directory. If the agent can provision IMS users in the future, the provisioning action will not happen immediately because polling is periodic.

It is not necessary to provision IMS users because Encentuate IAM Enterprise can now be configured to skip the sign up process for new users.

Strong Authentication Setup

This chapter covers the following topics:

- [Encentuate password setup](#)
- [ActiveDirectory password setup](#)
- [USB Key setup](#)
- [OTP Token setup](#)
- [Mobile ActiveCode setup](#)
- [RFID setup](#)
- [Active RFID setup](#)
- [Fingerprint setup](#)
- [Multiple second factor support setup](#)

Encentuate password setup

During sign-up (or first logon, for a provisioned user), a user is asked to specify the Encentuate password. The user also must specify a secret by choosing one from a list of questions (`pid_bind_secret_question_list`) and providing the answer to it. The secret is typically information not easily forgotten by user, is permanent in nature, and is not easily made known to others.

This secret is usually used in exceptional situations such as password reset. It is used for authenticating the user when password is not available, so that Administrator cannot access a user's credentials by resetting his password.

If registration of self-service secrets is enabled (`pid_secrets_register_for_selfhelp_at_sign_up`), the user can choose to specify more secret questions and answers, which can be used by the self-service feature for password reset or bypass of second factor.

ActiveDirectory password setup

The complete list of policies for Active Directory password synchronization can be found in the appendix (See [Policies](#)). Some policies have a Notes section that indicate their dependencies and relationships with other policies.

Recommended settings

- Enable the Encentuate password aging policy (**pid_enc_pwd_periodic_change_enabled**) and set it such that Encentuate password expires earlier than Active Directory password (**pid_enc_pwd_change_days** and **pid_enc_pwd_expiry_change_enforced**). This is to ensure that personal desktop and laptop users do not see the Active Directory password expiry screen during logon to desktop, as Encentuate password will expire first and that will trigger an Active Directory password change internally.

However, during the first setup there is still a chance that Active Directory password expires first. If this happens, the user will still see the Windows change password dialog. User must enter old and new password. AccessAgent will capture the new Active Directory password and trigger an Encentuate password change at IMS Server.

- Set **pid_ad_verification_on_logon_option** to **2** for computers that have joined the Active Directory domain, and to **0** for computers that do not join the Active Directory domain (e.g., home computers).
- It is recommended that **pid_automatic_sign_up_enabled** should be set to **1**.
- Modify **pid_logon_credentials_text** and **pid_unlock_credentials_text**, if desired.

Using the IMS Configuration Utility, set the **Synchronize user password with the password in the enterprise directory?** option in the enterprise directory settings to **Yes**. See [Setting up a new enterprise directory](#) for more details on Enterprise Directory configuration.

Additional information

- The "sign up", "change password" and "reset password" workflows always require the computer to have joined the appropriate Active Directory domain. However, the logon workflow can be configured (**pid_ad_verification_on_logon_option**) to skip password verification with Active Directory. This option is required as the user may sometimes log on to AccessAgent at home, which is not on the logon domain.

- Encentuate password strength policies (`pid_enc_pwd_min_length`, `pid_enc_pwd_max_length`, `pid_enc_pwd_min_numerics_length`, `pid_enc_pwd_min_alphabets_length`, `pid_enc_pwd_mixed_case_enforced`) will not be effective if Active Directory password synchronization is enabled since the Active Directory password complexity rules will be enforced instead.
- Active Directory password synchronization cannot be used in a USB Key deployment.

USB Key setup

USB Key is the recommended second factor for personal workstations.

To install the USB Key as a second factor:

- 1 Install AccessAgent.
- 2 Set `pid_second_factors_supported_list` to USB.

By default, Windows would show the contents of a removable drive in an Explorer window when plugged into a computer. Since the USB Key contains a removable drive, this would happen whenever user plugs it into a computer to log on, which may not be desirable. To disable this Windows feature, refer to the tip in [Enabling/Disabling autoplay for removable drives](#).



USB Keys do not work on Windows 2000 machines with USB 2.0 hubs (internal or external).

If there are USB Key detection problems (e.g., AccessAgent takes a long time to detect USB Key after resuming from standby or hibernation), modify the number of attempts and frequency of retries during Key detection.

These settings are configured through registry values under the `[HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\SOCIAccess\USB\Detection]` registry key.

Registry Value Name	Value Data (DWORD)	Description
ExplicitUSBHubRefreshEnabled	1 0 (default: 0)	Whether AccessAgent should explicitly refresh the USB Hub in the device tree. Note that this causes issues on some machines, while it might be necessary to do this on specific machines.

Registry Value Name	Value Data (DWORD)	Description
FlashDetectionAttemptCount	Min 2 Max unlimited (default: 5)	Number of attempts that AccessAgent goes through to detect the Flash using the Windows Plug and Play (PnP) service.
FlashDetectionAttemptIntervalMsecs	Min 100 Max unlimited (default: 200)	Sleep time in msecs between attempts to detect the Flash using PnP.
SCardDetectionAttemptCount	Min 5 Max unlimited (default: 10)	Number of attempts that AccessAgent goes through to detect the Smart Card using PCSC.
SCardDetectionAttemptIntervalMsecs	Min 50 Max unlimited (default: 200)	Sleep time in msecs between attempts to detect the Smart Card using PCSC.
SCardPKCSDetectionAttemptCount	Min 2 Max unlimited (default: 5)	Number of attempts that AccessAgent goes through to detect the Smart Card using PKCS11 (Axalto API).
SCardPKCSDetectionAttemptIntervalMsecs	Min 100 Max unlimited (default: 500)	Sleep time in msecs between attempts to detect the Smart Card using PKCS11.
SCardPingerEnabled	1 0 (default: 1)	Whether to enable the Smart Card pinger. The pinger has been suspected of causing certain machines to hang.
SCardPingerIntervalMins	Min 1 Max 10 (default: 3)	Interval, in mins, between consecutive Smart Card pings.



The policy settings can be set using AccessAdmin.

For more information on turning off auto-play on removable drives, see [Enabling/Disabling autoplay for removable drives](#) in [Deployment Tips](#).

OTP Token setup

To support the use of OTP token for authentication, an application must be configured to use IMS Server as the RADIUS authentication server. This is similar to configuring an application to use MAC or other forms of OTP for authentication.

Deployment options

An enterprise application that uses OTP tokens for authentication should prompt the user for a user name and password, where the password can be the Encentuate password, or an application password (e.g., Active Directory password).

For the second factor, the enterprise application can be configured to authenticate users with:

- Only OTP provided by token.
- Either OTP provided by token, or MAC.

The Administrator can also configure a bypass option, in case the user loses the OTP token or the mobile phone for receiving MAC.

The bypass code may be configured to be:

- Authorization code and Encentuate password
- Authorization code and enterprise account password
- Authorization code and secret

Workflow and use cases

The integrated product supports the following workflows and use cases:

- Uploading OTP token data files to IMS Server
- Registering users
- Assigning or revoking OTP tokens
- Searching for OTP tokens by serial number
- Authenticating users with OTP tokens
- Resetting OTP tokens

Uploading OTP Token data files to IMS Server

For an OTP token to appear in the list of unassigned tokens on AccessAdmin, it is necessary to upload the corresponding OTP data file to IMS Server first. This data file contains the OTP data and secrets for one token or an entire batch of tokens.

Uploading VASCO DPX files for VASCO Digipass

For each batch of Digipass tokens, VASCO provides a DPX file, which contains OTP-related secrets for each token in the batch. The DPX file is encrypted with an Encryption Key, which should also be provided by VASCO.

Before using a Digipass token, upload the information in its corresponding DPX file to the IMS Server. The command-line tool **upldDpx.bat** can be used to upload a DPX file to the IMS Server so that the entire batch of Digipass tokens will be recognized. Once uploaded, the tokens that correspond to the DPX file will appear in the list of unassigned tokens on AccessAdmin.

To use the command-line tool, go to the **ims\bin** subfolder of the IMS installation folder and issue the command:

```
upldDpx.bat [-i inputFileName] [-v] [-encryptKey encryptKey]
[-o outputFileName] [--error error-file] [-h] [-f folder]
[--overWrite option]
```

- **--error <error-file>**: Error output file name.
- **--encryptKey <encryptKey>**: Encryption Key for the DPX files.
- **-f, --folder <folder>**: Full path of the folder (include folder name) containing the DPX files for the given encryption key.
- **-h, --help**: Print help message.
- **-i, --input <inputFileName>**: Full path of the CSV file (include file name) for uploading multiple DPX files. Each row in the CSV file should be of the format "a,b", where a = Encryption Key, and b = Full path to DPX file (include DPX file name).
- **-o, --output <outputFileName>**: Output file name to which debug/output information is printed.
- **-v, --version**: Print version number of the tool.
- **--overWrite <option>**: Specifies if DPX information in the IMS Server for existing tokens in the unassigned list should be overwritten (turned off by default). <option> can be either **true** or **false**. If turned on, existing tokens (such as, tokens recognized by IMS Server) that do not appear in the DPX files, will not be modified. However, for existing tokens in the unassigned list, that appear in the DPX files, their DPX information in IMS Server will be overwritten with the ones in the DPX files.



Use the `--overWrite <option>` option when tokens go out-of-sync.

Uploading OATH Data files for Authenex A-Key

Each A-Key token uses an OATH seed to generate OTP. Before an A-Key token can be used, its serial number and OATH seed must be uploaded to IMS Server. The command-line tool **upldOath.bat** can be used to upload a CSV text file containing serial numbers and OATH seeds to IMS Server so that an entire batch of A-Key tokens will be recognized. Once uploaded, the tokens listed in the CSV file will appear in the list of unassigned tokens on AccessAdmin.

To use the command-line tool, go to the **ims\bin** subfolder of the IMS installation folder and issue the command:

```
upldOath.bat [-i inputFileName] [-o outputFileName] [-v] [-h]
```

- **-h**: Print help message.
- **-i <inputFileName>**: Full path of the CSV file (include file name) for uploading OATH data. Each row in the CSV file should be of the format "a,b", where a = Serial number of OATH token, and b = OATH seed of OATH token.
- **-o <outputFileName>**: Output file name to which debug/output information is printed.
- **-v**: Print version number of the tool.

Registering users

You can register a user using either of the following methods:

- The user signs up using AccessAgent.
- The user signs up through AccessAssistant or Web Workplace.
- The Administrator provisions the user with a user provisioning system that has been integrated with IMS Server.
- The Administrator registers the user with AccessAdmin (refer to the procedure).

To register a user using AccessAdmin:

- ① Log on to AccessAdmin.
- ② In the left panel, click **User registration**.

- ③ Search for the users to be registered.
- ④ For each user to be registered, click **Add>>** to add to the right-hand list.
- ⑤ Select the ActiveCode-enabled authentication services to be assigned to the users.
- ⑥ Click **Add Users** to register the selected users.

Assigning or revoking OTP Tokens

The Administrator or Helpdesk may assign an OTP token to a user or revoke it from the user.

To assign an OTP token to a user:

- ① Log on to AccessAdmin.
- ② Search for the user.
- ③ In the **OTP Token Assignment** section under the user's user profile, select a token from the list of unassigned tokens and click **Assign token**.

The assigned token will now appear as one of the user's authentication factors in the "Authentication Factors" section.

To revoke an OTP token from a user:

- ① Log on to AccessAdmin.
- ② Search for the user.
- ③ In the **Authentication Factors** section under the user's user profile, select the token and click **Revoke**.

The revoked token will now appear as one of the unassigned tokens in the **OTP Token Assignment** section.

Searching for OTP Tokens by serial numbers

The Administrator or Helpdesk can search for an OTP token by its serial number to identify the assigned user.

To search for an OTP Token by serial number:

- ① Log on to AccessAdmin.
- ② Enter the token's serial number followed by * from the **Search for:** field.
- ③ Select **OTP Token Serial Number** from the **Search by:** field.

- 4 Click **Search**.



If it is an unassigned token, the search will return the message, "No users matched the search criterion."

Authenticating users with OTP Tokens

For second factors, an enterprise application can be configured to authenticate user with:

- OTP only provided by token
- Either OTP provided by token, or MAC.

AccessAssistant and Web Workplace also offer users the choice of using a Helpdesk-issued authorization code as a second factor.

OTP only (time-based or OATH) enabled

If an enterprise application's authentication service is only enabled for **OTP (time-based)** or **OTP (OATH)** authentication (`pid_auth_authentication_option`), user authentication is as follows.

To authenticate users with OTP only enabled:

- 1 The user launches the application.
- 2 The user enters user name and password (Encentuate password or application password).
- 3 The IMS Server issues a RADIUS challenge for OTP.
- 4 The user enters OTP provided by the OTP token.
- 5 If the user lost the OTP token, the user can call Helpdesk for an authorization code. The user enters the authorization code followed by a secret (Encentuate password, enterprise account password, or user's secret) depending on `pid_activecode_bypass_option`.

Both OTP (time-based or OATH) and MAC enabled

If an enterprise application's authentication service is enabled for both **OTP (time-based)** or **OTP (OATH)** authentication and **MAC** authentication (`pid_auth_authentication_option`), user authentication is as follows.

To authenticate users with both OTP and MAC enabled:

- 1 The user launches the application.

- ② The user enters the user name and password (Encentuate password or application password).
- ③ The IMS Server issues an MAC and sends it to user's preferred MAC channel (Mobile ActiveCode preference).
- ④ The IMS Server issues a RADIUS challenge for MAC or OTP.
- ⑤ The user enters the MAC received by mobile phone or e-mail, or enters the OTP provided by the OTP token.
- ⑥ If the user lost both the mobile phone and OTP token, the user can call Help-desk for an authorization code. The user enters the authorization code followed by a secret (Encentuate password, enterprise account password, or user's secret), depending on **pid_activecode_bypass_option**.

AccessAssistant or Web Workplace

If AccessAssistant or Web Workplace is enabled for both **OTP (time-based)** or **OTP (OATH)** authentication and **MAC** authentication (**pid_auth_authentication_option** for **AccessAnywhere**), and two-factor authentication is enabled for the user (**pid_accessanywhere_second_factor_enabled**), user authentication is as follows.

To authenticate users with AccessAssistant or Web Workplace:

- ① The user launches AccessAssistant or Web Workplace.
- ② The user enters an Encentuate user name and password.
- ③ If the default second factor is MAC (**pid_accessanywhere_second_factor_default**), the IMS Server issues an MAC and sends it to user's preferred MAC channel (Mobile ActiveCode preference).
- ④ The user may enter the MAC received by mobile phone or e-mail, or enter the OTP provided by the OTP token.

Alternatively, the user can request for an MAC to be sent to another MAC channel.

- ⑤ If the user lost both the mobile phone and OTP token, the user can call Help-desk for an authorization code. The user enters the authorization code to log on.

Resetting time-based OTP Tokens

This workflow only applies to time-based tokens (e.g., VASCO Digipass). Since the VASCO Digipass is time-based, it usually does not go out-of-sync. However, according to VASCO documentation, a token can still be out-of-sync during exceptional circumstances (e.g., high temperature). If that happens, reset the OTP token (re-initialize) by uploading the DPX information using the upldDpx CLT.

To reset a time-based OTP Token:

- ❶ Revoke the tokens to move them to the unassigned list.
- ❷ Prepare a DPX file containing information for the reset tokens.
- ❸ Use the upldDpx CLT (see [Uploading VASCO DPX files for VASCO Digipass](#) section) with the **--overWrite true** option.
- ❹ Re-assign the tokens to users, if necessary.

Resetting OATH-based OTP Tokens

This workflow applies to OATH-based tokens (e.g., Authenex A-Key). Since the A-Key uses OATH OTP, which is event-based, the OTP can be out-of-sync with the IMS Server if the user presses the token button too many times (default 25) without using the displayed OTP for authentication. If that happens, reset the OTP token (re-synchronize) through either of the following ways:

- By the user, through AccessAssistant or Web Workplace.
- By the Administrator or Helpdesk, through AccessAdmin.

To reset an OTP token through AccessAssistant or Web Workplace:

- ❶ Log on to AccessAssistant or Web Workplace.
- ❷ Click the **Reset OTP token** link (`pid_accessanywhere_otp_reset_link_text`).
- ❸ Select the token's serial number.
- ❹ Generate three (`pid_otp_reset_sample_count`) consecutive OTPs using the token and enter each of them in the appropriate text boxes.
- ❺ Click **Reset**.

To reset an OTP token through AccessAdmin:

- ❶ Log on to AccessAdmin.
- ❷ Search for the user or OTP token.
- ❸ In the **Authentication Factors** section under the user profile, click the token's **Reset token** link.
- ❹ Generate three (`pid_otp_reset_sample_count`) consecutive OTPs using the token and enter each of them in the appropriate text boxes.
- ❺ Click **Reset**.

Installing OTP token support

This section contains installation and configuration instructions for OTP token support. It is assumed that an IMS Server has already been installed and configured.

The VACMAN Controller for Windows is in the VASCO installation package. There is no additional installation needed for Authenex.

Installing VASCO OTP library files

To use VASCO Digipass after installing the IMS server, you must manually install the required .DLL and .JAR files for VASCO OTP support in the IMS folders, since the IMS installer does not carry the .DLL and .JAR files.

To install VASCO OTP library files:

- ❶ Run the installer for VACMAN Controller for Windows.
- ❷ In the VACMAN Controller program files folder, search for **aal2sdk.dll** in the **win32\bin** subfolder and **aal2wrap.jar** in the **java\wrapper** subfolder.
- ❸ Copy the **aal2sdk.dll** and the **aal2wrap.jar** files to the IMS Server's **ims\WEB-INF\lib** folder.
- ❹ Restart the IMS Server.

Configuring RADIUS authentication for applications

To support OTP tokens for authentication, an application must be configured to use the IMS Server as the RADIUS authentication server. This is similar to configuring an application to use MAC or other forms of OTP for authentication.

Refer to the Remote Access Integration Guide for configuration details.

For AccessAssistant or Web Workplace, configuring RADIUS authentication is not required. The Administrator just sets the appropriate policies as indicated in the next section.

Enabling user registration through AccessAdmin

For customers that prefer to register their users through AccessAdmin, the following configuration should be done using the IMS Configuration Utility.

To configure the IMS server to allow user registration through AccessAdmin:

- ❶ Click **ActiveCode Deployment** in the left panel.
- ❷ Set **Mobile ActiveCode-only registration of users** to **true**.
- ❸ Set **Active Directory attribute to be displayed for Mobile ActiveCode-only registration of users user interface** to the desired Active Directory attribute (e.g., "displayName").
- ❹ Set **Search filter used for Mobile ActiveCode-only registration of users user interface** to the desired filter for the user search facility during user registration (e.g., "sAMAccountName=*").
- ❺ Click **Update**.
- ❻ Restart the IMS Server.

Setting ActiveCode-enabled authentication service bindings

Set the ActiveCode-enabled authentication service bindings for each user using an OTP token for a particular authentication service. This can be done through AccessAdmin by the Administrator or Helpdesk.

To set ActiveCode-enabled authentication service bindings:

- ❶ Log on to AccessAdmin.
- ❷ Search for the user.
- ❸ Click the **Authentication services** link for user.
- ❹ Under the **ActiveCode-enabled Authentication Services** section, select the authentication service.
- ❺ Enter the user name for the authentication service.
- ❻ Click **Add account**.

Alternatively, you can select the ActiveCode-enabled authentication services to be bound to the user during user registration through AccessAdmin.

The ActiveCode-enabled authentication services can also be automatically bound to the user once provisioned with a user provisioning system, or when signing up through AccessAgent, AccessAssistant, or Web Workplace. To enable the automatic-binding feature, configure the following configuration key in the **ims.xml** file in the **ims\config** folder:

```
<auth.otp.accountClasses>
```

```
<value xml:lang="en">dir_otp_app</value>

</auth.otp.accountClasses>
```

where `dir_otp_app` should be replaced by the authentication service ID. For AccessAssistant or Web Workplace, the authentication service ID is **AccessAnywhere**.

Policy settings

The recommended policy settings indicated here are for enabling OTP token use for authentication on AccessAssistant and Web Workplace using AccessAdmin.

For details on setting policies, see the Encentuate IAM Administrator Guide. Some policies have a **Notes** section that indicate their dependencies on and relationships with other policies.

User policy settings

Policy ID	Value
pid_wallet_sso_type_supported64	(OTP (time-based)) or 128 (OTP (OATH)) should be included in the list
pid_accessanywhere_second_factor_enabled	True

System policy settings

Policy ID	Value
pid_wallet_sso_type_supported	64 (OTP (time-based)) or 128 (OTP (OATH)) should be included in the list
pid_accessanywhere_second_factor_default	3 (OTP)
pid_otp_reset_sample_count (for Authenex A-Key only)	3
pid_accessanywhere_otp_reset_link_text (for Authenex A-Key only)	Reset OTP token

Authentication service policy settings

Policy ID	Value
pid_auth_authentication_option (for a specific authentication service, for example, "AccessAnywhere")	64 (OTP (time-based)) or 128 (OTP (OATH)) should be included in the list

Application policy settings

Policy ID	Value
pid_app_authentication_option (for a specific application)	64 (OTP (time-based)) or 128 (OTP (OATH)) should be included in the list

Advanced settings for OATH-based OTP

The following are advanced settings for OATH-based OTP that can be configured using the IMS Configuration Utility.

To set advanced settings for OATH-based OTP:

- 1 Launch the IMS Configuration Utility.
- 2 Go to **ActiveCode Deployment**.
- 3 Restart the IMS Server after changes are done.

OTP Look-Ahead Number

An OATH-based OTP token may not be completely in-sync with the IMS Server if the user presses the OTP token button without using the displayed OTP for authentication. This configuration key specifies the number of consecutive button presses that the user can make before the OTP token must be reset (re-synchronized). The default value is **25**.

OTP token reset window

When an OATH-based OTP token is reset, the IMS Server attempts to re-synchronize with the OTP token by computing a series of consecutive OTPs until it finds a match with the three consecutive OTPs generated by the OTP token.

This configuration key specifies the maximum number of OTPs that the IMS Server will try during a single reset attempt. If the IMS Server fails to reset an OTP token, this number must be increased. The default value is **100**.

Issues and notes

Take note of the following Entenuate IAM Enterprise support details for OTP token:

IMS installer does not carry VASCO libraries

The IMS installer does not carry the DLL and JAR files required for VASCO OTP support. For more information, see [Installing VASCO OTP library files](#).

Application name appended to serial number for Digipass

For each Digipass token, the serial number uploaded to the IMS database also contains the application name. However, the application name does not appear in the serial number printed on the back of the actual token.

If an Administrator or Helpdesk personnel searches for a Digipass token on AccessAdmin by serial number, the Administrator or Helpdesk must enter the serial number, followed by "*" in the search text so AccessAdmin can find the token.

Mobile ActiveCode setup

An Encentuate Mobile ActiveCode is a one-time password (OTP) that is randomly generated and event-based. The Mobile ActiveCode is generated on the IMS Server and delivered through second channel such as text services (Short Message Service) on mobile phones. It is used for strong authentication.

To deploy the Encentuate MAC solution:

- ❶ Install the IMS Server. For setup details, see the Encentuate IAM Administrator Guide.
- ❷ Configure MAC settings at IMS Server. For setup details, see [Configuring MAC Settings at IMS Server](#).
- ❸ Configure message connector settings at IMS Server. For setup details, see [Configuring a message connector](#).
- ❹ Provision users at IMS Server using the AccessAdmin interface. For setup details, see [Configuring MAC Settings at IMS Server](#).
- ❺ Enable MAC settings for applications and users at IMS Server. For setup details, see [Enabling MAC for Applications and Users](#).



If you need to authenticate MAC for an application, see [Integrating an Application with MAC Using SOAP API](#).

- ❻ End user workflows may change, depending on whether you are deploying a full Encentuate IAM Enterprise solution, or the application logon interface is customizable. For details, refer to the next sections.

For RADIUS applications, for example, VPN:

- ❼ Configure the RADIUS interface at the IMS Server. For setup details, see [Configuring the RADIUS Interface at IMS Server](#).
- ❽ Configure the VPN Server to re-direct authentication. For setup details, see either of the following: [Integrating with Aventail SSL VPN](#), [Integrating with Juniper SSL VPN](#), or [Integrating with F5 SSL VPN](#).

For non-RADIUS applications:

- 7 Develop an Encentuate IMS Bridge using the published Encentuate SOAP API for MAC. For details, refer to [Integrating an Application with MAC Using SOAP API](#).

RFID setup

To install an RFID reader:

- 1 Run the installer for the appropriate reader.
 - For the GIGA-TMS Proximity Readers PCR105MU and PCR300MU, install the PL-2303 driver on the client machine by running PL-2303 Driver Installer.exe in the **PL2303** folder.
 - For the Altrus RFID Reader, install the PL-2303 driver on the client machine by running PL-2303 Driver Installer.exe in the **PL2303** folder.
 - When the GIGA-TMS Proximity Reader MFR135 is plugged in for the first time, install the driver by asking making a Windows search in the **GIGAMFR135_DRIVERS\MFR135** folder.
- 2 Install AccessAgent.
- 3 Set **pid_second_factors_supported_list** to **RFID**.



This policy can be set using AccessAdmin.

- 4 Set the CardType registry setting in AccessAdmin [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\SOCIAccess\RFID] according to the following table:

Card Type	CardType (DWORD)
Cards with HID standard IDs (All Prox cards and iCLASS cards	0
Mifare cards with 32-bit CSN	1
Mifare cards with greater than 32-bit CSN	2
Notes: This class of cards includes iTag.	

This setting indicates the RFID card type used in a deployment. Only one category of RFID card is supported per deployment. If a wrong category of RFID cards is used, the serial number for each card may be read as different values across different models of readers.

For example, if CardType is set to 0 and a Mifare card is being read, a GIGA-TMS Proximity Reader PCR300MU would return a different CSN from that returned by a GIGA-TMS Proximity Reader MFR135.

This setting is necessary because Mifare cards, in general, can be uniquely distinguished by a CSN, while the Prox cards are uniquely distinguished by Building Access Numbers (facility code + employee ID). iCLASS cards have both in them, and depending on which reader is used, one of them is read.

- ❶ For GIGA-TMS and Altrus readers, set the ReaderType, ComPort, and ReaderString registry settings in [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\SOCIAccess\RFID\Mifare] according to the following table:

Reader	ReaderType (DWORD)	ComPort (DWORD)	ReaderString (REG_SZ)
GIGA-TMS Proximity Reader MFR135 (PCMCIA reader for Mifare cards)	0	0	PROMAG
GIGA-TMS Proximity Reader PCR300MU (USB reader for Mifare cards)	0	0	Prolific
Altrus Mifare Desktop Reader Writer A1 (USB reader for Mifare cards)	2	0	Prolific
GIGA-TMS Proximity Reader PCR105MU (USB reader for Mifare cards)	3	0	PROMAG

The ReaderString setting is case-sensitive.

The ComPort should be set to 0 for the reader models, for AccessAgent to automatically search for the correct COM port. For troubleshooting, you can determine the reader COM port (specific to a machine) by plugging in the reader and checking the Ports (COM & LPT) entry in the Device Manager of Windows.

The policy settings can be set using AccessAdmin.



iTags (Mifare smart labels) should be pasted on hard surfaces as far as possible. It has been observed that label detection deteriorates after a while if the labels are bent during usage.

Active RFID setup

To install an ARFID reader:

- ❶ Run **setup.exe** to install the XyLoc Service on the client machine.

- ② When the XyLoc Lock is plugged in for the first time, Windows will search for the driver in the **xyloc_setup\drivers** folder and install the driver.
- ③ Install AccessAgent.
- ④ Set **pid_second_factors_supported_list** to ARFID.



The policy can be set using AccessAdmin.

The North American and European versions of the XyLoc Keys and Locks use different frequency ranges. North American Keys can only work with North American Locks, and European Keys can only work with European Locks.

- North American versions are indicated with "FCC" on the Lock and "RF Band: North America" on the Key.
- European versions are indicated with "CE" on the Lock and "RF Band: Europe" on the Key.

Line of sight between Key and Lock is preferred for XyLoc to work optimally. Water can significantly reduce the signal strength, and any body part may block the radio signal (e.g., folding your arms over the Key, or walking away with your back facing the Lock). Metallic objects can block or reflect the radio signal.

The Lock should not be placed on or near metallic objects. If it must be placed on a metallic surface, it must be shielded with a thick non-metallic object. Note that cordless phones using the 900MHz range in the US may interfere with the North American version of XyLoc. Such interference may reduce the signal range significantly.

Ensure Technologies recommends that the Lock and Key should be placed at around the same level. If the Lock is mounted on the monitor, then the Key should be around the upper part of the body.

The distance is not the issue, but rather the possibility for other things to affect the RF signal, such as the desk, the body, the keyboard, etc. All these things affect signal strength. Even a user's arm passing in front of the Key can cause the signal to drop slightly.

Refer to Ensure's Lock positioning demo: <http://www.ensuretech.com/support/documentation/movies/lockpositionlowres.mpg>

The battery should last for 9 to 12 months on average (Keys issued before September 2006 have an average life span of one year). The age of the battery should not adversely affect signal strength as this kind of battery tends to maintain a rather constant power throughout its life span until the final one or two weeks.

XyLoc is currently working on including a battery weak notification in its server user interface, so Administrators can be informed of users with weak batteries. To conserve battery life, Keys automatically turn off after 13.5 hours (Keys issued

before September 2006 have an operating time of 9 hours). To extend the 13.5 hours operating time, press the **O** ON button for each extra hour needed, up to a maximum of 16.5 hours.

The XyLoc Service has a logging feature that is useful for troubleshooting. Set **Logging** to **1** in [HKEY_LOCAL_MACHINE\SOFTWARE\Ensure Technologies\XyLoc]. Restart the **XyLoc Security System** service.

The logs are stored in **C:\Program Files\Ensure Technologies\XyLoc**. Each packet that is sent from any Key in the vicinity is logged. Each Key sends two packets per second, one from each antenna (there are 2) of each Key. The logs indicate the Key-ID as well as signal strength received by the Lock.

If AccessAgent has been installed before installing XyLoc Service, the appropriate registry settings can be manually set as follows after installing the XyLoc Service:

- ❶ Locate [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SOCI-Access] key in the registry.
- ❷ Add **XyLoc Security System** as a string to the **DependOnService** multi-string value.
- ❸ Restart the machine.

ARFID detection ranges can be configured as either machine or system policies. For more information on setting policy priorities, see [Setting policy priorities](#). See [Definitions of policies](#) for detailed definitions of the ARFID policies. Note the following:

- There is a recommended value for each policy.
- The minimum difference between **pid_arfid_presentation_range_max** and **pid_arfid_removal_range_min** is **3**. If the difference between the two is set to less than **3** AccessAgent reverts to the default values (3 and 7).
- It is not advisable to use values as high as **13** and **14**, since at those values, an increment of **1** (from 13 to 14) corresponds to a considerably small change in actual signal strengths. This can result in inconsistent behavior from the XyLoc Service, and consequently from AccessAgent as well.
- When the ARFID range policies are changed, the new values are in effect if you perform a synchronization with IMS Server (for system policies), and then lock and unlock the computer.

Fingerprint setup

To install DigitalPersona readers:

- ❶ On IMS Server, install Java Runtime Environment 1.3.1 and above, as well as the U.are.U Integrator Gold Sensor Software for Java (run `SETUP.EXE` in the **DP Gold frsw 2.5\Fingerprint Recognition SW for Java** folder).
- ❷ On IMS Server, install the U.are.U Integrator Gold Sensor Software (run `SETUP.EXE` in the **DP Gold frsw 2.5\Fingerprint Recognition SW** folder). The machine restarts automatically after the software is installed.
- ❸ Configure IMS Server for biometrics support using the IMS Configuration Utility.
- ❹ On the client machine, install AccessAgent.
- ❺ On the client machine, install the U.are.U Integrator Gold Sensor Software (run `SETUP.EXE` in the **DP Gold frsw 2.5\Fingerprint Recognition SW** folder). The machine restarts automatically after the software is installed.
- ❻ Set `pid_second_factors_supported_list` to **Fingerprint**. The policy can be set using AccessAdmin.

On some machines, it has been observed that the U.are.U Integrator Gold Sensor Software must be re-installed when AccessAgent is upgraded. Basically, the Sensor Software must be installed after AccessAgent installation. In such cases, be sure that the machine policy is set properly using AccessAdmin.

On some Windows Server 2000 and Windows Server 2003 machines, it has been observed that the U.are.U Integrator Gold Sensor Software fails to install these two files in the Windows System32 folder: **dpDevDat.dll**, and **dpDevCtl.dll**.

If these are missing, there will be lookup errors on IMS Server when it tries to use DigitalPersona services.

To fix the problem, copy these files from another machine with the U.are.U Integrator Gold Sensor Software installed, and then restart the DigitalPersona and IMS Server services.

The installer for the DigitalPersona software for Java does not detect JRE 1.6. An error would be encountered during installation: "Java Runtime Environment 1.3 or later is required." If this happens, download an older version of JRE from Sun and try again.

For installations (UPEK configuration only, for AccessAgent version 3.2.1.12 and above, and IMS Server version 3.1.7.1 and above) on the IMS Server, install the UPEK BioAPI SDK (run `TCKDU06B.exe` in the **UPEK** folder) before installing the IMS Server software. When prompted, select all features except SDK for installation.

To install the UPEK configuration (for AccessAgent version 3.2.1.12 and above, and IMS Server version 3.1.7.1 and above) on the IMS Serve:

- ❶ On the client machine, install the UPEK BioAPI SDK (run `TCKDU06B.exe` in the **UPEK** folder). When prompted, select all features except SDK for installation.
- ❷ On the client machine, install AccessAgent.
- ❸ Set **pid_second_factors_supported_list** to **Fingerprint**. This policy can be set using AccessAdmin.

Due to limitations of the UPEK BioAPI SDK, if AccessAgent is installed on the same machine as the IMS Server. AccessAgent must be disabled for fingerprint authentication by setting the following fingerprint device-related registry entries to 0:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\SOCI-Access\DSPList\{090A055B-04B9-44B9-A6AF-8D523B95799C}]"Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\SOCI-Access\DSPList\{C9E4F95D-3E9F-47AF-B556-95DD27C8ADDA}]"Enabled"=dword:00000000
```



IMS Server version 3.1.7.1 cannot be used with AccessAgent version 3.2.0.6 or earlier. Similarly, AccessAgent version 3.2.1.12 or later cannot be used with IMS Server 3.1.5.4 or earlier.

The UPEK fingerprint sensor is very sensitive. User has to swipe finger very carefully, and at a reasonable speed--not too slow or too fast. Press finger firmly against sensor, especially towards the fingertip end while swiping.

With AccessAgent version 3.3.0.0 and above, and IMS Server version 3.3.0.0 and above, you can register more than one finger (depends on **pid_fingerprint_registration_max**). You can then use any of the registered fingers to log on to AccessAgent. As such, if IMS Server is upgraded from a version below 3.3.0.0, the CLT, **addFpType.bat** (in **<IMS Installation Folder>\ims\bin**), should be run to convert all users' fingerprint data.

If fingerprint authentication is used on a shared workstation, it is recommended that the limit on the number of cached Wallets (**pid_wallet_cache_max**) be set to a value such that the possibility of false acceptance for the fingerprint device is made negligible. This is because false acceptance may lead to a user logging on to a wrong Wallet.

If a limit on the number of cached Wallets is set, inactive Wallets should be set to expire on IMS Server (using **pid_wallet_cache_max_inactivity_days**) and revoked accordingly.

If both UPEK and DigitalPersona support are needed on an IMS Server, make sure that the DigitalPersona SDK is installed before the UPEK SDK. The SDK installers are known to cause problems if UPEK is installed before DigitalPersona.

Multiple second factor support setup

To install fingerprint and RFID on one workstation:

- ❶ Install AccessAgent for Fingerprint support (see [Fingerprint setup](#)).
- ❷ Set `pid_second_factors_supported_list` to **Fingerprint** and **RFID** (in that order) if AccessAgent is to prompt for fingerprint during sign up. Set `pid_second_factors_supported_list` to **RFID** and **Fingerprint** (in that order) if AccessAgent is to prompt for RFID card during sign up.



This policy can be set using AccessAdmin.

- ❸ If desired, set the configurable text policies for simultaneous Fingerprint and RFID support:

```
pid_engina_logon_with_fingerprint_or_rfid_text,  
pid_unlock_with_fingerprint_or_rfid_option_1_text,  
pid_unlock_with_fingerprint_or_rfid_option_3_text,  
pid_unlock_with_fingerprint_or_rfid_option_4_text
```

The supported sign up workflow is as follows:

- The user can click the **Sign up** link from EnGINA welcome screen, locked screen, or user desktop. Alternatively, the user can attempt to log on using an unregistered user name, and proceed to the sign up workflow as well. Besides the password and secret, the user will be asked to present an RFID card or fingerprint, depending on whether **RFID** or **Fingerprint** appears first in `pid_second_factors_supported_list`.
- The user may also tap an unregistered RFID card at EnGINA welcome screen, locked screen, or user desktop. Sign up with RFID card will be initiated regardless of whether **RFID** appears first in `pid_second_factors_supported_list`.

The user may also present an unregistered finger at EnGINA welcome screen, or user desktop. Sign up with fingerprint will be initiated regardless of whether **Fingerprint** appears first in `pid_second_factors_supported_list`.



From the locked screen, you cannot sign up by presenting a finger.

The supported second factor registration workflow is as follows:

- An existing user can tap an unregistered RFID card or present an unregistered finger at EnGINA welcome screen, locked screen, or user desktop. Registration of the new second factor will proceed as usual regardless of whether **RFID** or **Fingerprint** appears first in `pid_second_factors_supported_list`.

The supported logon workflow from a locked screen is as follows:

- From the workstation, User A chooses either a fingerprint or RFID reader.
- User A places a finger on the fingerprint reader.
- If authenticated, the user is logged on using a single factor.
- If authentication fails, User A is prompted to register the fingerprint. The user can click **Log on** to try logging on again using password or RFID card.
- From the workstation, User B chooses either a fingerprint or an RFID reader.
- User B taps the RFID card and enters the password, and is authenticated with 2 factors.
- If the RFID card is not registered, User B is prompted to register the RFID card. The user can click **Log on** again using password or fingerprint.
- If User B has forgotten to bring the RFID card, the user can place a finger on the fingerprint reader and be authenticated with 1 factor.

Take note of the following information on multiple second factor support:

- AccessAgent does not check whether a reader is physically present or not. Hence, `pid_second_factors_supported_list` has to be set appropriately.
- AccessAgent does not allow registering both RFID card and fingerprint during signup. Users who need to register both will have to register them separately.
- If the user enters a user name and password to log on, but the Wallet authentication policy allows only **Fingerprint** logon, the user cannot log on and will receive a message to place a finger on the fingerprint reader.



*It is advisable to enable both **Password** and **Fingerprint** logon for each user's Wallet authentication policy, as both are single-factor authentication.*

-
- User signup is not supported from the locked screen for fingerprint authentication, but AccessAgent supports fingerprint registration from a locked screen for existing users.
 - AccessAgent allows registering of fingerprint or RFID card even if a user's Wallet authentication policy does not allow him to use any of them for logon.



Deploying both fingerprint and RFID readers on a workstation might be complicated. Users may not know where to tap RFID cards or place their fingers. This is more challenging when the user has only an RFID card or fingerprint registered, but some computers only have one of the readers. Users must be trained to minimize Helpdesk support calls. Control the second factor usage to minimize context-switching for users. Retain the user's preferred authentication factor.

AccessAssistant and Web Workplace Setup

With AccessAssistant and Web Workplace, enterprises can enjoy single sign-on without the hassle of deploying AccessAgent to client PCs, as long as enterprise applications are all Web-based.

The Web automatic sign-on feature gives users the ability to log on to enterprise Web applications by simply clicking on links on AccessAssistant, Web Workplace, or enterprise portals, without the need to remember the passwords for individual applications. Users will just need to remember a single password to log on to all applications. Combined with the reverse proxy feature, Web automatic sign-on is able to support a very large variety of Web applications.

If AccessAgent is not deployed, users would have to sign up through other means. The enterprise can choose to integrate an identity provisioning system with Encentuate IAM Enterprise and provision users using it. Alternatively, users can sign up with Encentuate IAM Enterprise through AccessAssistant or Web Workplace.

Just like signing up through AccessAgent, users would need to authenticate themselves by providing their enterprise directory password (e.g., Active Directory password) first, and then specify the Encentuate password and secret. Users can optionally choose to specify more secret questions and answers, which can be used by the self-service feature for password reset.

AccessAssistant and Web Workplace offer a host of self-service capabilities to the users. Users who usually use AccessAgent to log on to enterprise applications may need to know the application passwords when they use PCs that do not have AccessAgent installed. AccessAssistant allows users to view their application passwords or copy them to clipboard.

Users can also reset their secret questions and answers through AccessAssistant or Web Workplace. Instead of having to call Helpdesk for an authorization code, the self-service feature allows users to reset their Encentuate passwords by providing a subset of the secrets that they have previously specified.

Users of AccessAgent will find the user interfaces of AccessAssistant and Web Workplace familiar because they have been designed to minimize the need for user training.

For each user, the Wallet that can be accessed through AccessAgent, AccessAssistant, or Web Workplace is the same. The contents are fully synchronized across the user interfaces. System, machine, and user policies are all configured through AccessAdmin, making it easy for Administrators to configure all user interfaces from one central console.

AccessAssistant enables users to view application passwords, whereas Web Workplace does not. Its UI has been designed to facilitate the viewing of application passwords. On the other hand, Web Workplace's UI has been designed to look like a typical portal page. This will facilitate logging on to enterprise Web applications. It can be integrated with the customer's existing portal or SSL VPN, and AccessAssistant will perform such an integration.

This chapter covers the following topics:

- [Installing AccessAssistant and Web Workplace](#)
- [Deploying AccessAssistant or Web Workplace.](#)
- [Upgrading AccessAssistant and Web Workplace](#)
- [Embedding Web Workplace in the enterprise portal](#)
- [Managing policies](#)
- [Setting automatic Web sign-on for AccessProfiles](#)

Installing AccessAssistant and Web Workplace

There are two ways to install AccessAssistant and Web Workplace:

- with IMS
- without IMS

To install AccessAssistant and Web Workplace with IMS:

Install the IMS Server.

To install AccessAssistant and Web Workplace without IMS:

The following are in the installation package:

- .WAR files: **AccessAssistant.war** and **WebWorkplace.war**

- **accessAnywhere.properties** file (in config folder).

This is the configuration file for both AccessAssistant and WebWorkplace. The configuration key `WEB_WORKPLACE_ENABLED` needs to have the value "enabled" for Web Workplace.

Make sure that the IMS server name is also correctly set.

- **web_aa_sync_data.xml** file (in config folder): Default Web AccessProfiles.

These AccessProfiles are already uploaded to IMS Server by default. However, if the IMS Server is upgraded from a previous version that does not contain these AccessProfiles, the file can be uploaded by using the "upldSync" IMS command-line tool: `upldSync --dataFile web_aa_sync_data.xml`.



web_aa_sync_data.xml contains AccessProfiles that can only be interpreted by WebWorkplace and not by AccessAgent.

- **web_aa_sync_data_test.xml** (in config folder): Sample Web AccessProfiles.

These AccessProfiles are not uploaded to IMS Server by default. The file can also be uploaded by using the "upldSync" IMS command-line tool: `upldSync --dataFile web_aa_sync_data_test.xml`

- **canned_pages** folder: Folder containing default pre-stored logon forms (canned pages) for Web automatic sign-on.

Deploying AccessAssistant or Web Workplace.

To deploy AccessAssistant or Web Workplace in the same Tomcat instance that the IMS Server is running in:

- ❶ Stop the IMS Server.
- ❷ Edit both `runserver.bat` in `<IMS Installation Folder>\ims\bin` folder and `installService.bat` in `<IMS Installation Folder>\ims\bin\installer` folder to include the system property: `accessAnywhere.configFile` specifies the location of the `accessAnywhere.properties` file.

For example: `set JAVA_OPTS=%JAVA_OPTS% -DaccessAnywhere.configFile=%CATALINA_HOME%\accessAnywhere.properties`

- ❸ In a command prompt, go to the `<IMS Installation Folder>\ims\bin\installer` folder and run `installService changeit` where `changeit` is the keystore password.

④ Copy the WAR file to **<IMS Installation Folder>**.

⑤ Start **IMS Server**.

An AccessAssistant or WebWorkplace folder should be automatically created within **<IMS Installation Folder>**.

For IMS Server versions lower than 3.5.0, the following must be done to auto-deploy the WAR file before starting the IMS Server:



1. Modify **server.xml** in **<IMS Installation Folder>\conf** folder.

2. Under the tag `<Engine Name="StandAlone" defaultHost="localhost" debug="0">`, look for the "Host" tag and change the entries for **unpackWARS**, **autoDeploy** and **liveDeploy** to "true" as indicated: `<Host name="localhost" debug="0" appBase="/" unpackWARS="true" autoDeploy="true" liveDeploy="true">`

To deploy AccessAssistant or Web Workplace (another Web server):

- ① Stop the Web server where AccessAssistant or Web Workplace is going to be deployed.
- ② Import the remote IMS Server's SSL certificate to the Web server's Java trust store.
- ③ The trust store location is specified by the system property: `javax.net.ssl.trustStore`.
- ④ The trust store password is specified by the system property: `javax.net.ssl.trustStorePassword`.
- ⑤ The location of `accessAnywhere.properties` is specified by the system property: `accessAnywhere.configFile`.
- ⑥ Modify **server.xml** in **conf** folder. Under the tag `<Engine Name="StandAlone" defaultHost="localhost" debug="0">`, look for the "Host" tag and change the entries for **unpackWARS**, **autoDeploy** and **liveDeploy** to "true" as indicated: `<Host name="localhost" debug="0" appBase="/" unpackWARS="true" autoDeploy="true" liveDeploy="true">`
- ⑦ Copy the .WAR file to the **webapps** folder.
- ⑧ Start the Web server that is hosting the .WAR file.

An AccessAssistant or WebWorkplace folder should be automatically created.

AccessAssistant and Web Workplace settings

Ensure that the **accessAnywhere.properties** file has been specified correctly as follows:

- The **accessAnywhere.properties** file can be found in the **config** folder, which is placed alongside the .WAR file.
- The location of the **accessAnywhere.properties** file is specified by the system property **accessAnywhere.configFile**. If that is not found, search the classpath for the properties file.
- The **config** folder can be placed anywhere in the system as long as the system property **accessAnywhere.configFile** points to the path where **accessAnywhere.properties** can be found.

To edit the accessAnywhere.properties file:

- ❶ Modify the key: **IMS_SERVER_HOSTNAME** should contain the hostname of IMS Server.
- ❷ Modify any other keys, as appropriate.
- ❸ Restart the IMS Server or the hosting Web server for any configuration changes to take effect.

Upgrading AccessAssistant and Web Workplace

To upgrade AccessAssistant or Web Workplace:

- ❶ Copy the **accessAnywhere.properties** file from the existing installation and save it somewhere for use later.
- ❷ Delete the existing **AccessAssistant** or **WebWorkplace** folder.
- ❸ Install the WAR file according to instructions.
- ❹ Reinstate the **accessAnywhere.properties** file that was saved in the first step.
- ❺ Restart the IMS Server or hosting Web server for the changes to take effect.

Embedding Web Workplace in the enterprise portal

This feature allows users to perform automatic sign-on to a Web application through Web Workplace from a link in the enterprise portal.

For each Web application embedded in the enterprise portal, use a URL of the form: https://WebWorkplace/link_auto_logon.jsp?&acctClass=authserviceid&appName=appid&refresh=true

where:

- WebWorkplace is the URL of Web Workplace.
- authserviceid is the authentication service ID to be used.
- appid is the application ID of the application.

The following is an example link: https://preview.encentuate.com/WebWorkplace/link_auto_logon.jsp?&acctClass=dir_yahoo&appName=app_yahoo_web&refresh=true

Managing policies

This sections contains all the policies relevant to AccessAssistant and Web Workplace using AccessAdmin.

For details on setting policies, see the Encentuate IAM Administrator Guide. Some policies have a **Notes** section that indicate their dependencies on and relationships with other policies.

For more information on the recommended policy settings for enabling OTP token use for authentication on AccessAssistant and Web Workplace using AccessAdmin, see [Policy settings](#) in [Strong Authentication Setup](#).

User policy settings

Policy ID	Value
pid_accessanywhere_enabled	True
pid_accessanywhere_second_factor_enabled	(depends on customer preference)
pid_accessanywhere_second_factor_default	(depends on customer preference)
pid_accessanywhere_personal_app_enabled	(depends on customer preference)

System policy settings

Policy ID	Value
pid_accessanywhere_session_timeout_mins	10
pid_accessanywhere_password_display_secs	60
pid_accessanywhere_edit_user_profile_enabled	True
pid_accessanywhere_app_sso_enabled	True
pid_accessanywhere_sync_mins	30
Note: This policy is temporarily disabled due to some issues. Administrator will have to manually perform synchronization with IMS Server by logging on to AccessAssistant or Web Workplace and clicking on the "Synchronize system data with IMS Server" link. This is required when there are changes to any of the system policies listed in this section.	
pid_accessanywhere_password_display_option	2 (Display password by default, with option to copy to clipboard)
pid_selfhelp_password_reset_enabled	True
pid_secrets_register_for_selfhelp_max	3
pid_secrets_verify_for_selfhelp	2
pid_secrets_verify_invalid_trial_count_max	6
pid_secret_id_reveal_at_verify_failure	False

Setting automatic Web sign-on for AccessProfiles

An Administrator can author and manage Web AccessProfiles from AccessAssistant or Web Workplace. The following additional options are available for Administrators:

- **Manage AccessProfiles:** To view, add, modify, or test Web AccessProfiles.
- **Synchronize system data with IMS Server:** To synchronize AccessProfiles and system policies with the IMS Server.

There are two types of Web AccessProfiles:

- **Dynamic AccessProfile**

This type of Web AccessProfile uses the reverse proxy feature. It can be used for virtually all kinds of Web applications.

■ Static AccessProfile

Web AccessProfiles that do not use the reverse proxy feature are static AccessProfiles. It typically uses a pre-stored logon form for logging on to the Web application.

The set of Web applications that can be supported by static AccessProfiles is a subset of those supported by dynamic AccessProfiles. However, we recommend the use of static AccessProfiles as far as possible because such AccessProfiles impose much less load on the AccessAssistant or Web Workplace server than dynamic ones.

To create a Web AccessProfile:

- ❶ Create a static AccessProfile for the application.
- ❷ Test the static AccessProfile.

Or:

- ❶ Create a dynamic AccessProfile for it.
- ❷ Test the dynamic AccessProfile.

Or:

Use the above processes by modifying the other parameters for the AccessProfile.

For detailed descriptions of AccessProfiles and related concepts, refer to the AccessStudio User Guide.

Use the AccessAssistant and Web Workplace wizard to maintain existing, and create Web AccessProfiles.

Maintaining existing AccessProfiles

To maintain existing AccessProfiles:

- ❶ Click **Manage AccessProfiles** from the navigation pane. This displays the Manage AccessProfiles screen.

Manage AccessProfiles screen

- 2 Click the application link to set up the application's AccessProfiles.

Modifying AccessProfiles



Click **Download AccessProfile** to view the AccessProfile scripts.

- 2 Specify the details for your AccessProfile.

AccessProfile ID

Enter the ID which is usually prefixed with "web_sso_site_".

Logon page URL

Enter the application logon page URL. Dynamic AccessProfiles should prefix the actual logon URL with "https://\$IMS_SERVER\$/\$AAWWP\$/rproxy/fetch/" where \$IMS_SERVER\$ refers to the IMS server domain and \$AAWWP\$ refers to the path where AccessAssistant/Web Workplace is deployed.

URL prefix

Enter the URL prefix that should be applied to all relative links in the logon page. This is only used for dynamic AccessProfiles.

Use pre-stored logon form

Select **true** from the dropdown menu if you want to use pre-stored logon form. Otherwise, logon page will be retrieved dynamically.

Use cookies for logon

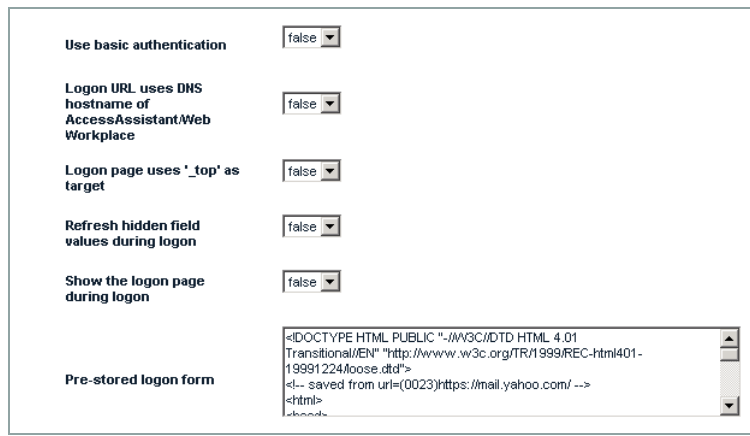
Select **true** if you want the logon page to use cookies for a faster logon process. If not, select **false**.

Use basic authentication

Select **true** from the dropdown menu if you want the logon page to use HTTP basic authentication scheme. Otherwise, select **false**.

Logon URL uses DNS hostname of AccessAssistant/Web Workplace

Select **true** from the dropdown menu if you want the application's logon page to have the same DNS hostname as AccessAssistant/Web Workplace. Otherwise, select **false**.



The screenshot shows a configuration window titled "Modifying AccessProfiles". It contains several settings, each with a label and a dropdown menu set to "false":

- Use basic authentication
- Logon URL uses DNS hostname of AccessAssistant/Web Workplace
- Logon page uses '_top' as target
- Refresh hidden field values during logon
- Show the logon page during logon

At the bottom, there is a text area labeled "Pre-stored logon form" containing the following HTML code:

```
<!DOCTYPE HTML PUBLIC "-//W3C/DTD HTML 4.01 Transitional/EN" "http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd">
<!-- saved from url=(0023)https://mail.yahoo.com/ -->
<html>
<head>
```

Modifying AccessProfiles

Logon page uses '_top' as target

Select **true** from the dropdown menu if you want the application's logon page to use '_top' as target window. This prevents the page from being displayed within a frame. Otherwise, select **false**.

Refresh hidden field values during logon

Select **true** from the dropdown menu if you want hidden fields of pre-stored logon form to be refreshed on each logon. This is applicable only if pre-stored logon form is used. Otherwise, select **false**.

Show the logon page during logon

Select **true** from the dropdown menu if you want the logon page to be visible when the username/password is auto-filled. Otherwise, select **false**.



Pre-stored logon form is the application's logon form stored in AccessAssistant/WebWorkplace. It is only applicable if the **Use pre-stored logon form** is set to **Yes**.

Authentication service	Yahoo!		
Application	Yahoo web		
Account data template	adt_ciuser_cspwd		
User name field	Frame	name	
	Form	name	login_form
	Field	name	login input text
Password field	Frame	name	
	Form	name	login_form
	Field	name	passwd input password

Modifying AccessProfiles

Authentication services

Select the authentication service for this AccessProfile from the dropdown menu. An authentication service can be created using AccessStudio or IMS Server Configuration. See Creating an authentication service in the AccessStudio Guide for details.

Application

Select the application for this AccessProfile from the dropdown menu. An application can be created using AccessStudio or IMS Server Configuration. See Creating an application object in the AccessStudio Guide for details.

Account data template

Select the account data template of the authentication service from the dropdown menu. See Account data items and templates in the AccessStudio Guide for details.

User name field

For the user name signature, specify the frame, form, field, and input type, where applicable.

Password field

For the password signature, specify the frame, form, field, and input type, where applicable.

OK button	Frame	name	
	Form	name	login_form
	Field	name	.save input text
<div>Update Delete</div>			

Modifying AccessProfiles

OK button

For the **OK** button, specify frame, form, field, and input type, where applicable. The **OK** button is the signature of confirmation control.

- 3 Click **Update** once you are done with the configuration. Otherwise, click **Delete**.

Creating Web AccessProfiles

To create a Web AccessProfiles:

- 1 Click the **Add Access Profile >** button.
- 2 Go through the basic configuration.

Step 1: Basic Configuration [< Back](#)

The following steps will guide you through the configuration of the AccessProfile for your application. Begin by providing basic configuration information.

Logon page URL

Authentication service [Create new authentication service](#)

Application [Create new application](#)

Account data template

Steps 2 to 6 will generate a static AccessProfile, which is recommended, but it may not work for some applications. If you would like to create a dynamic AccessProfile, you may skip the steps below and proceed to [Step 7](#).

Creating new AccessProfiles

1. Enter the URL of the application logon page. Dynamic AccessProfiles should prefix the actual logon URL with "https://\$IMS_SERVER\$/ \$AAWWP\$/rproxy/fetch/" where \$IMS_SERVER\$ refers to the IMS server domain and \$AAWWP\$ refers to the path where AccessAssistant/Web Workplace is deployed.
2. Select an authentication service for this AccessProfile from the Authentication service dropdown menu. If what you need is not in the dropdown menu, click **Create new authentication service** to create one. It can also be created using AccessStudio or IMS Server Configuration. See Creating an authentication service in the AccessStudio Guide for details.
3. Select an application for this AccessProfile. If what you need is not in the dropdown menu, click **Create new application**. You can also create an application using AccessStudio or IMS Server Configuration. See Creating an application object in the AccessStudio Guide for details.
4. Select an account data template for the authentication service. See Account data items and templates in the AccessStudio Guide for details.

- 3 Click **Download logon page**.

Step 2: Download logon page

Download the logon page into a Helper browser window by clicking on the button below.

Creating new AccessProfiles

- 4 Click **Extract logon form**.

Step 3: Extract logon form

Extract the logon form from the Helper browser window by clicking on the button below. This is the logon form that will be pre-stored.

Creating new AccessProfiles

- 5 Click **Load logon form**.

Step 4: Load logon form

Load the extracted logon form into the Helper browser window by clicking on the button below.

Creating new AccessProfiles

- 6 Click **Generate test signature**.

Step 5: Generate test signature

Generate a test signature for the logon form by clicking on the button below. User name and password fields will be automatically identified.

Creating new AccessProfiles

- 7 Click **Proceed to test**. Once you are done, Click **Go to final step**. Then click **Create dynamic AccessProfile**.

Step 6: Test

Test the above signature by clicking on the button below. A test user name and password should be submitted into the Helper browser window.

Did you see the test user name and password being submitted into the Helper browser window? If not, you may want to go back to Step 2 to modify the logon form or test signature and try testing again, or you may choose to try creating a dynamic AccessProfile. If OK, proceed to final step.

Creating new AccessProfiles

- 8 Click **Download logon page**.

Step 7: Download logon page

The following steps will guide you through the configuration of a dynamic AccessProfile for your application. First, download the logon page into the Helper browser window by clicking on the button below.

Creating new AccessProfiles

- 9 Click **Generate test signature** to test the dynamic AccessProfile.

Step 8: Generate test signature for dynamic AccessProfile

Generate a test signature for the logon form by clicking on the button below. User name and password fields will be automatically identified.

Creating new AccessProfiles

- 10 Click **Proceed to test**. Once you are done, click **Go to final step**.

Step 9: Test

Test the above signature by clicking on the button below. A test user name and password should be submitted into the Helper browser window.

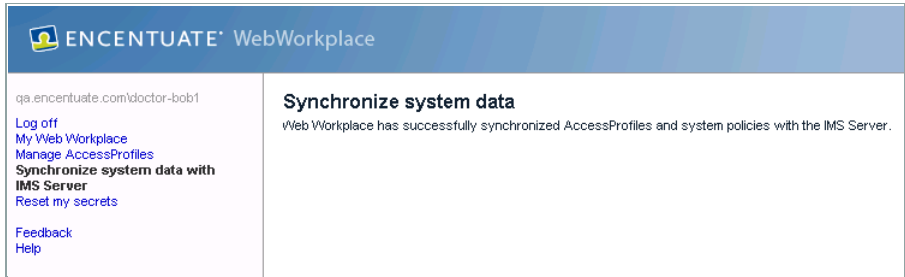
Did you see the test user name and password being submitted into the Helper browser window? If not, you may want to go back to Step 7 to modify the test signature and try testing again, or you may choose to try creating a dynamic AccessProfile. If OK, proceed to final step.

Creating new AccessProfiles

- 11 After the tests, in **Final Step: Upload AccessProfile**, the Administrator can modify any of the fields, as needed. If the generated settings generated are satisfactory, click **Upload to IMS Server** to complete AccessProfile generation.

Synchronizing system data with the IMS Server

Click the **Synchronize system data with IMS** link from the navigation panel to upload the changes to IMS.



Synchronizing system data with IMS

PART III: MONITORING AND MANAGEMENT

Part III: Monitoring and Management

Use this part of the guide to learn more about setting up internal and external monitoring systems to integrate with Encentuate IAM Enterprise. Refer to the following chapters:

- [Microsoft Operations Manager \(MOM\)](#), which provides instructions on importing, installing, and setting up MOM to integrate with the IMS Server.
- [SNMP and JMX Support](#), which contains instructions on installing AdventNet JMX-SNMP on IMS Server, setting up IMS Server to support SNMP and JMX, and testing the SNMP and JMX functionalities on IMS Server.
- [Auditing and Reporting](#), which lists internal tools to help users monitor activity in Encentuate IAM Enterprise, such as event logs, database views, logon/logoff tracking, and setting up custom events.

Microsoft Operations Manager (MOM)

Microsoft Operations Manager (MOM) is the event and performance management element of the Microsoft's Windows Server System. The product allows monitoring of numerous computers interconnected by one or more communications networks.

Many Microsoft server products, such as Active Directory, Microsoft SQL Server, Microsoft Exchange Server, and MOM itself can be monitored through MOM. MOM began as a network management system developed by NetIQ, a provider of integrated systems and security management solutions, and later was acquired by Microsoft in 2000.

Integrating the IMS Server with MOM provides customers with a unified monitoring and management solution across the entire corporate platform. MOM allows Administrators to examine the health status of the IMS Server and trigger alerts when certain important events occur.

This chapter covers the following topics:

- [About MOM](#)
- [Importing the MOM Management Pack for the IMS Server](#)
- [Installing the MOM agent on the IMS Server](#)
- [Setting up IMS Server logging for Syslog](#)

About MOM

MOM depends on agents to manage computers. An agent is a piece of software running on managed computers to monitor system resources, for example, a Windows event log. Specific events or alerts can be generated by applications running on the monitored computer. Upon event occurrence and detection, MOM agents forward the event to a central MOM server.

The MOM server maintains a history of events in a database by applying filtering rules to all incoming events and generating the necessary notifications. A notification can take the form of an e-mail, a pager message, a network support ticket, or some other workflow intended to correct the problem that triggered the notifications.

Several MOM servers can be aggregated to monitor multiple networks across logical Windows domains and physical network boundaries. Through a connector framework scheme employing Web services, individual MOM servers can exchange alerts with other network management applications.

MOM uses the term "Management Pack" to refer to a set of filtering rules, knowledge, and public views specific to some monitored application. Management Packs serve as a container and distribution vehicle that MOM uses to deploy the configuration information required for managing computers and applications.

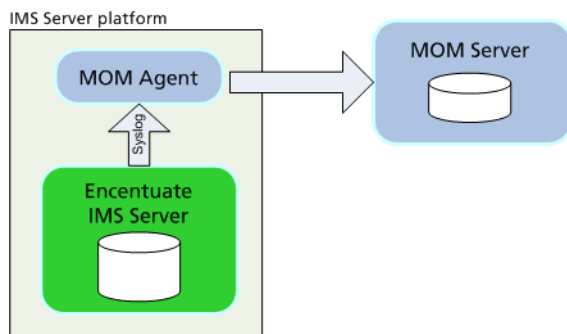
While Microsoft and other software vendors make Management Packs available for their products, MOM also provides facilities for authoring custom Management Packs. A MOM Management Pack for IMS Server (in AKM file format) has been developed to make it easy for system Administrators to integrate IMS Server with MOM.

The integration of Encentuate IAM Enterprise with MOM allows Administrators to monitor the health status of IMS Server and to examine Encentuate IAM Enterprise event logs through the MOM console. The IMS Server has to be set up to transmit event logs to an MOM agent (running on the same server machine) through a Syslog protocol.

In turn, the MOM agent filters the received logs based on pre-defined rules and sends the filtered events to the MOM server for storage. The MOM agent also monitors the system resources (e.g., Windows event log, memory, and CPU) and notifies the MOM Server based on the defined rules.

The MOM server maintains a history of events in a database by applying filtering rules to all incoming events and generating notifications whenever necessary. A notification can be sent through e-mail, a pager message, a network support ticket, or some other workflow.

The next diagram illustrates the integration between the IMS Server and MOM.



Integrating IMS Server with MOM

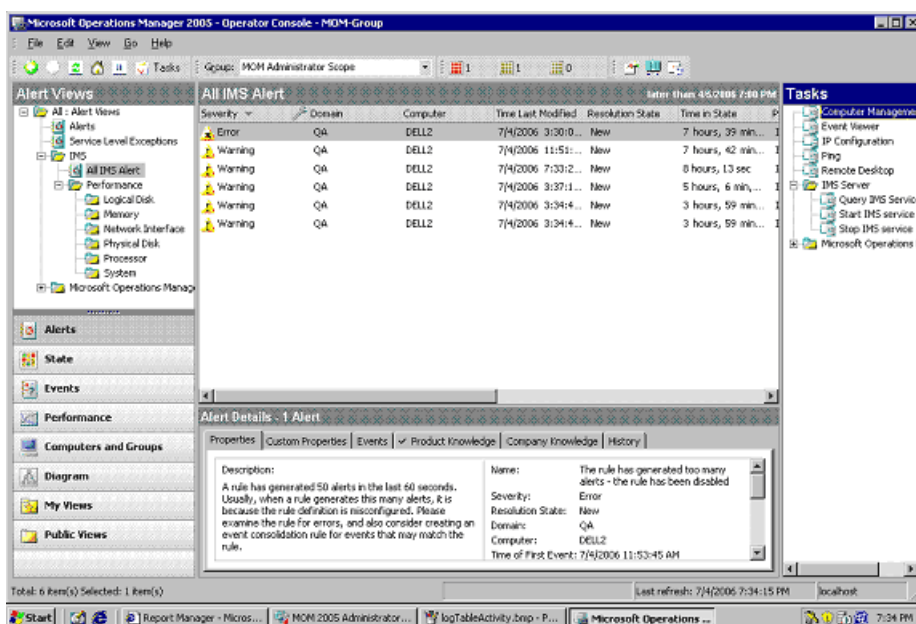
Monitoring the IMS Server health status

Using the MOM Operator console, Administrators can monitor the health status of each IMS Server, and check whether the server is up or down. The console can also show performance monitoring graphs for various health parameters of the IMS Server, including:

- CPU utilization
- Memory utilization
- Disk utilization
- Page file utilization
- Context switches per second
- CPU queue length

Starting or stopping the IMS Server from the MOM console

The Administrator can start or stop IMS Server using the MOM Operator console.



MOM Operator Console Alert View

Storing audit logs in the MOM server

The Administrator chooses which IMS Server log tables (user activity, system management activity, etc.) are exported to the MOM server through the Syslog protocol.

To reduce the size of the IMS Server database, the Administrator can also configure the IMS Server to export the logs to the MOM server without storing them in the IMS Server database. This can improve the performance of the IMS Server.



At present, logs sent to external entities through Syslog protocol are not tamper-evident. Once Administrators abort the IMS Server database logging in favor of MOM-managed audit logging and reporting, reporting log tampering is effectively lost.

Triggering alerts based on rules

The MOM server can generate alerts or notifications based on rules applied to IMS Server health information, including audit logs received from the IMS Server.

Audit reports using MOM reporting tools

The MOM server uses two databases (DB) – one for live operations, and the other for archival. Activity events are transferred from the live DB to the archival DB every night. Reports can be generated from:

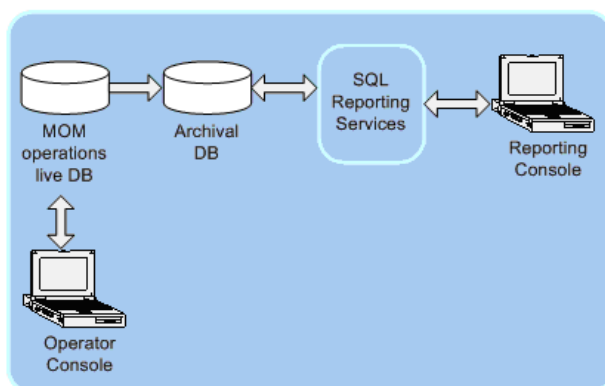
- Reporting console, using SQL Reporting Services, based on archival data
- Operator console based on live data

However, the data sources cannot be combined to produce reports.

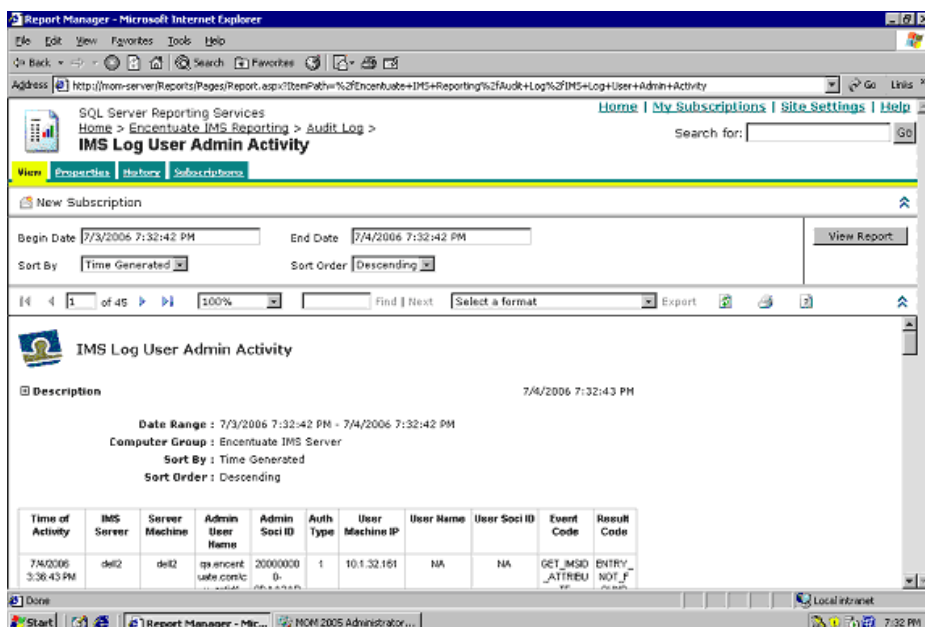
The MOM Management Pack for IMS Server includes XML schemas for SQL Reporting Services, so standard reports can be generated from the MOM reporting console.



At present, logs sent to external entities through Syslog protocol are not tamper-evident. Once Administrators abort the IMS Server database logging in favor of MOM-managed audit logging and reporting, reporting log tampering is effectively lost.



MOM Reporting Options



MOM Reporting Console

Importing the MOM Management Pack for the IMS Server

To import the MOM Management Pack for the IMS Server, launch the MOM Administrator console. Right-click on *Management Packs >> Import/Export Management Packs*. Then, select the type of import to perform.

MOM prerequisites

The supported version of MOM is Microsoft Operations Manager 2005 with Service Pack 1

MOM 2005 requires the following:

- Microsoft SQL Server 2000 with Service Pack 3a or above
- Microsoft.NET Framework version 1.1

IMS Server prerequisites

The following are pre-requisites for installing the MOM agent on the IMS Server machine:

- Windows Installer 3.1 and above is required
- DCOM is enabled (next procedure)

To enable DCOM:

- ❶ Open **dcomcnfg** in *Start >> Run*.
- ❷ Navigate to *Console Root >> Component Services >> My Computer*.
- ❸ Right-click on **My Computer** and select **Properties**.
- ❹ In the **My Computer Properties** dialog box, select **Default Properties** tab.
- ❺ Make sure the **Enable Distributed COM on this computer** option is enabled.

Installing the MOM agent on the IMS Server

Use the MOM Administrator console to install the MOM agent on the IMS Server.

To install the MOM agent on the IMS Server:

- ❶ Navigate to *Console Root >> Microsoft Operations Manager (SERVER_NAME) >> Administration >> Computers >> Agent-managed Computers*.
- ❷ Click *Action >> Install/Uninstall Agents Wizard*.
- ❸ Select **Install Agents**, and click **Next**.
- ❹ Search for the IMS Server, and click **Next**.
- ❺ Specify the Administrator account to use for the installation, and click **Next**.
- ❻ Specify the Agent Action Account to use for collecting data, and click **Next**.
- ❼ Specify the Agent installation directory, and click **Next**.
- ❽ Click **Finish** to complete the installation.
- ❾ The IMS Server should appear in the list of Agent-managed Computers (you may need to refresh the list).

Setting up IMS Server logging for Syslog

To send logs to the MOM agent using Syslog protocol, configure the IMS Server, using the IMS Configuration Utility.

To set up the IMS Server logging for Syslog:

❶ Go to *Advanced Settings >> IMS Server >> Logging >> Syslog*.

❷ Specify the necessary settings.

Syslog enabled

Add the log tables to be stored in MOM server.

Syslog server port

The MOM agent's Syslog server port should be 514.

Syslog server hostname

Use IMS Server's hostname.

Syslog logging facility

The Syslog facility code should be 20.

Syslog field-separator

The Syslog message field separator is set to \n by default. But for MOM reporting, it must be set to ;.

❸ Click **Update**.

❹ Go to *Advanced Settings >> IMS Server >> Logging >> Log Server Information*.

❺ For **Log server type**, add **syslog** to the list. If logging to the IMS Server database will be disabled, remove **rdb** from the list.



If logging to the IMS Server database is disabled, the links for displaying Logs and Reports in AccessAdmin will be hidden.

❻ Click **Update**.

❼ Restart the IMS Server.

SNMP and JMX Support

The IMS Server is an integrated management system that provides a central point of secure access administration for an enterprise. It interfaces with many other systems, such as application servers and messaging gateways.

The ability to check security status, performance, and availability of the IMS Server is critical to the success of a customer's business. Deploying the IMS Server in a distributed environment without comprehensive management solutions runs the risk of losing productivity and affecting security.

The recent integration of the IMS Server with Microsoft Operations Manager (MOM) provides MOM customers with a unified monitoring and management solution across the entire corporate platform. MOM allows Administrators to examine the health status of the IMS Server and triggers alerts when events occur.

However, MOM only collects operating system health status information and audit logs sent by the IMS Server. MOM cannot look inside Tomcat, JVM, or IMS Server for health information such as **number of open sessions**, **request processing time**, and **number of DB errors**.

There are also many customers using various brands of Network Management Systems (NMS) or Enterprise Systems Management solutions, such as IBM Tivoli, CA Unicenter, HP OpenView, and BMC Patrol. Most of these systems already support SNMP and/or JMX for monitoring and managing network objects.

If the IMS Server supports SNMP and JMX, it can be monitored and managed by a variety of NMS systems. At the same time, the health status of Tomcat and JVM can also be exposed to such systems.

This chapter covers the following topics:

- [About SNMP](#)
- [About JMX](#)
- [SNMP and JMX system requirements](#)
- [Installing AdventNet JMX-SNMP Adaptor on the IMS Server](#)
- [Setting up IMS Server for SNMP and JMX support](#)
- [Testing SNMP and JMX](#)

About SNMP

The Simple Network Management Protocol (SNMP) is a long-existing protocol for central monitoring and management of network objects (applications, servers, routers, etc.).

Traditional, NMS or Enterprise Systems Management solutions, like IBM Tivoli, CA Unicenter, HP OpenView and BMC Patrol all support SNMP.



Microsoft MOM provides limited support to SNMP (SNMP traps only).

However, the IMS Server and its underlying platform (Tomcat 4.1, Sun JVM 1.4.2) do not natively support SNMP, because Java applications support JMX as its monitoring and management mechanism.

SNMP's extensible design is achieved with management information bases (MIBs), which specify the management data of a device subsystem, using a hierarchical namespace containing object identifiers, implemented via ASN.1.

The MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organizations. This model permits management across all layers of the OSI reference model, extending into applications such as databases, e-mail, and the J2EE reference model, as MIBs can be defined for all such area-specific information and operations.

The different versions of SNMP are SNMPv1, SNMPv2c, and SNMPv3. SNMPv1 is the first version of the protocol. SNMPv2c is the revised protocol, which includes enhancements of SNMPv1 in the areas of protocol packet types, transport mappings, MIB structure elements but using the existing SNMPv1 administration structure ("community based" and hence SNMPv2c).

The latest standard, SNMPv3, defines a secure version of SNMP. It also facilitates remote configuration of the SNMP entities. Although SNMPv3 is already quite widely supported (Cisco IOS, Sun Management Center, HP OpenView, IBM Tivoli NetView, BMC Patrol, CA Unicenter), customer adoption is unknown. Sun JVM 1.5 natively supports SNMPv2c, which is also supported by virtually all NMSes.

For maximum leverage with minimum effort, the IMS Server will support SNMPv2c first. Support for SNMPv3 will be considered in the future when there is a demand.

About JMX

Java Management Extensions (JMX) is a Java technology that supplies tools for managing and monitoring applications, system objects, devices (e.g., printers), and service oriented networks. An interesting detail of the API is that classes can be dynamically constructed and changed.

JMX uses a proprietary TCP/IP protocol to communicate with various devices in your intranet or on the Internet. The application server running the servlets will offer various methods that allow inquiry of the state of the device and to obtain detailed information, such as usage, logging information, or error texts.

A typical System Management tool uses a JMX heartbeat message to verify that the distributed devices are healthy. The heartbeat message invokes a method on the remote application servers and receives a response.

A managed bean (MBean) is an object that one can access via JMX, some or all JavaBean properties and possibly call "operations" which are basically just normal methods. It usually represents a manageable resource, such as an application, a service, a component, or a device.

SNMP and JMX system requirements

IMS Server and its underlying platform (Tomcat 4.1, Sun JVM 1.4.2) do not natively support SNMP. This is because Java applications support JMX as its monitoring and management mechanism.

The JMX attributes are exposed through SNMP using a commercially available JMX-SNMP adaptor (by AdventNet). In this way, the same set of IMS Server system attributes can be monitored by both SNMP and JMX compatible NMSes.

This section describes the high-level specifications of the feature.

SNMP support

SNMPv2c is supported.

Customers can monitor and configure IMS Server via SNMP compatible products, such as IBM Tivoli NetView and HP OpenView.

JMX support

JMX is supported.

Customers can monitor and configure IMS Server via JMX compatible products like Sun Java Monitoring and Management Console (JConsole), and HP OpenView.

Monitor IMS Server, Tomcat, and JVM

NMSes should be able to monitor health information and receive notifications from the JVM, Tomcat, or IMS Server, via SNMP or JMX.

Information to be monitored

- All the attributes available in Sun JVM 1.4.2's native JMX support.
- All the attributes available in Tomcat 4.1's native JMX support.

The IMS Server attributes that can be monitored are grouped into four types or categories:

- **certAuthority:** Attributes pertaining to IMS Server CA.
- **config:** Attributes pertaining to IMS Server configuration keys. These are the same attributes that can be set using the IMS Configuration Utility.
- **dataObject:** Attributes pertaining to IMS Server database and log database.
- **runtime:** Attributes pertaining to IMS Server runtime status and operations.

The four tables below describe the available attributes for each type. Each type is mapped to a corresponding SNMP name, which is exposed by the JMX-SNMP adaptor. The SNMP names are indicated in the tables below too.

Type: certAuthority SNMP name: imsCertAuthority	
Attribute Name	Description
DistinguishedName	Distinguished name (DN) of the CA
ExpiryDate	Expiry date of the CA root certificate Notes: <i>The AdventNet JMX-SNMP adaptor currently does not support the conversion of JMX date object. Hence, this attribute is not available through SNMP.</i>
RemainingDays	Number of days before the CA root certificate expires
JssVersion	JSS version of the CA
NsprVersion	NSPR version of the CA
NssVersion	NSS version of the CA
TokenName	Token name of the CA

Type: config SNMP name: imsConfig	
Attribute Name	Description
AllConfigKeys	List of all IMS configuration keys
AllConfigSubSections	List of all IMS configuration sub-sections
ConfigStore	IMS configuration file

Type: dataObject SNMP name: imsDataObject	
Attribute Name	Description
DbConnectionsUsed	Number of database connections currently in use
DbErrorCount	Number of database errors since server started
ImsDbPoolSize	IMS database pool size
LogDbPoolSize	Log database pool size

Type: runtime SNMP name: imsRuntime	
Attribute Name	Description
ImsVersion	IMS Server version
StartTime	IMS Server start time
UpTime	IMS Server uptime (in milliseconds)
ServerSessionsCount	Current number of active IMS sessions
ActiveThreads	Current number of active threads
FreeMemory	Current amount of free memory
ActiveCodeLoginFailureCount	Number of failed ActiveCode logins since server started
ActiveCodeLoginSuccessCount	Number of successful ActiveCode logins since server started
ActiveCodeLockoutCount	Number of ActiveCode lock-outs since server started
PasscodeLoginFailureCount	Number of failed local logins since server started
PasscodeLoginSuccessCount	Number of successful local logins since server started
ScrLoginFailureCount	Number of failed SCR logins since server started
ScrLoginSuccessCount	Number of successful SCR logins since server started
LogSevereCount	Number of severe log entries since server started
LogWarningCount	Number of warning log entries since server started
ServiceAttemptFailureCount	Number of failed service attempts since server started
ServiceAttemptSuccessCount	Number of successful service attempts since server started
WalletLockoutCount	Number of Wallet lock-outs since server started

IMS Server notifications

- Failure to connect to DB
- Failure (of application connector) to connect to external directory/application
- Failure (of message connector) to connect to messaging gateway
- Very high DB connection count
- Very high ActiveCode logon failure rates
- Wallet lock-out
- ActiveCode lock-out

Installing AdventNet JMX-SNMP Adaptor on the IMS Server

This section contains installation and configuration instructions for enabling SNMP and JMX support. It is assumed that an IMS Server has been installed and configured.

JMX support is included in the basic IMS Server installation, but not SNMP, as the AdventNet JMX-SNMP Adaptor must be purchased by the customer from AdventNet.

To install the AdventNet JMX-SNMP Adaptor:

- ❶ Copy the files **AdventNetSnpAdaptor.jar** and **AdventNetSnpAdaptor-Framework.jar** into the **<IMS Installation Folder>\ims\WEB-INF\lib** folder.
- ❷ Copy the **\conf** folder into the **<IMS Installation Folder>\ims\config** folder (such as, creating a **conf** folder in the **config** folder).

Setting up IMS Server for SNMP and JMX support

To set up IMS Server for SNMP and JMX support using the IMS Configuration Utility:

- ❶ Launch the IMS Configuration Utility.
- ❷ Go to **Advanced Settings >> IMS Server >> SNMP**.

- 3 Specify the following settings.

JMX HTTP port number

Specify the port number of the HTTP adaptor for JMX, if the HTTP interface for JMX is enabled.

JMX HTTP Login

Specify the login user name for the HTTP adaptor for JMX, if the HTTP interface for JMX is enabled.

JMX HTTP Password

Specify the password for the HTTP adaptor for JMX, if the HTTP interface for JMX is enabled.

JMX JRMP port number

Specify the port number of the JRMP adaptor for JMX, if the JRMP interface for JMX is enabled.

JMX JRMP Login

Specify the login user name for the JRMP adaptor for JMX, if the JRMP interface for JMX is enabled.

JMX JRMP Password

Specify the password for the JRMP adaptor for JMX, if the JRMP interface for JMX is enabled.

- 4 Click **Update** and restart the IMS Server for the configuration changes to take effect.

Testing SNMP and JMX

The tools described in this section can be used to test the SNMP and JMX setup.

Using the JMX HTTP Adaptor

If the JMX HTTP adaptor is enabled, it can be accessed via a Web browser at **http://imsserver:port** where **imsserver** is the IMS Server hostname and **port** is the port number configured for the JMX HTTP adaptor.



The JMX HTTP adaptor does not support notification at the moment. To see JMX notifications, use the MC4J control panel.

Using the AdventNet MibBrowser tool

To test the SNMP adaptor:

- ❶ Install the AdventNet SNMP tools.
- ❷ Run the **MibBrowser** software.
- ❸ Load the MIB file provided in the <IMS Installation Folder>\ims\config\conf folder.
- ❹ Enter the IMS Server IP address or hostname in the Host box.
- ❺ Use **8001** as the default SNMP port.
- ❻ Operational details of the tool can be read from the online help file.

Testing the MC4J software

To test the MC4J Management Console if the JMX JRMP adaptor is enabled:

- ❶ Download, install, and run the **MC4J Management Console** software (see <http://mc4j.org>).
- ❷ Create a new server connection.
- ❸ Select **MX4J 1.x** as the server connection type.
- ❹ Make sure that the server URL is pointing to IMS Server with the configured port (e.g., `rmi://imsserver:9090`, where "imsserver" is the IMS Server hostname and "9090" is the port number configured for the JMX JRMP adaptor).
- ❺ Further help for the tool can be found at the MC4J website.

Auditing and Reporting

One of the strengths of Encentuate IAM Enterprise is its comprehensive identity auditing framework. The identity information and events captured in the database allow Administrators to generate useful reports for identity auditing, such as:

- List of application accounts for a user
- Policy changes performed by an Administrator or Helpdesk on a user
- Successful and failed application logons and logoffs
- Summary table of the number of times each user logs on to each application within a period of time

This chapter covers the following topics:

- [Viewing the event log](#)
- [Generating database views](#)
- [Tracking successful/unsuccessful logons and logoffs](#)
- [Creating custom events](#)

Viewing the event log

Each action is captured as an event in the audit logs. Each event is accompanied by a result code. The description of each event or result code can be obtained from IMS Server at the URL: <https://imsserver/ims/ui/diagnostics>. Log on first to AccessAdmin before navigating to the page.

Generating database views

A collection of database views are available for Administrators to generate useful identity auditing reports using some SQL query tool (e.g., Microsoft SQL Query Analyzer, Crystal Reports, etc.).

Tracking successful/unsuccessful logons and logoffs

Encentuate IAM Enterprise can track successful/failed logon and logoff for all enterprise applications as part of audit logs. This feature can be turned on as long as the AccessProfile for each application implements the action `acc_data_audit_log_action`:

```
<acc_data_audit_log_action>

  <!--account data bag id-->

  <acc_data_bag_id use_local_bag="1">default_injection_bag</
acc_data_bag_id>

  <!--event code in decimal-->

  <event_code>1107296303</event_code>

  <!--result code for event: 0 for success and 1 for failure-->

  <return_code>0</return_code>

</acc_data_audit_log_action>
```

Use the following event codes:

- 1107296303: Authentication service logon
- 1107296304: Authentication service logoff

These two events can be searched via the Logs feature on AccessAdmin. For each user, the audit log history should also show these two events. If the logon/logoff event is successful, the result for the event will be displayed as **OK**, otherwise it will be shown as **Error**.

For old versions of AccessStudio, this action has to be manually added to each AccessProfile. This action can be added after an inject/capture action in the same trigger with the account data bag id being the one used in the earlier action. In the following example, four audit log actions have been added after the inject action which executes when the logon window appears:

```

<wnd_activate_trigger>

    <signature>/child::wnd[@title="Logon to Training App"]</
signature>

    <next_state_id>state_after_inject</next_state_id>

    <actions>

        <action>

            <acc_data_inject_action>

                <acc_data_bag id="default_injection_bag">

                    </acc_data_bag>

                    <sso_items>

                        </sso_items>

                        <auth_info>

                            <direct_auth_info>

                                <auth_id>dir_training_app</auth_id>

                                </direct_auth_info>

                            </auth_info>

                        </acc_data_inject_action>

                    </action>

                    <action>

                        <acc_data_audit_log_action>

                            <!-- this indicates user has successfully logged
on -->

                                <acc_data_bag_id>default_injection_bag</
acc_data_bag_id>

                                <event_code>1107296303</event_code>

                                <return_code>0</return_code>

                                </acc_data_audit_log_action>

                            </action>

                            <action>

                                <acc_data_audit_log_action>

```

```

                                <acc_data_bag_id>default_injection_bag</
acc_data_bag_id>

                                <!-- this indicates user has failed to log
on -->

                                <event_code>1107296303</event_code>

                                <return_code>1</return_code>

                                </acc_data_audit_log_action>

                                </action>

                                <action>

                                    <acc_data_audit_log_action>

                                        <acc_data_bag_id>default_injection_bag</
acc_data_bag_id>

                                        <!-- this indicates user has successfully logged
off -->

                                        <event_code>1107296304</event_code>

                                        <return_code>0</return_code>

                                        </acc_data_audit_log_action>

                                    </action>

                                    <action>

                                        <acc_data_audit_log_action>

                                            <acc_data_bag_id>default_injection_bag</
acc_data_bag_id>

                                            <!-- this indicates user has failed to log off
-->

                                            <event_code>1107296304</event_code>

                                            <return_code>1</return_code>

                                            </acc_data_audit_log_action>

                                        </action>

                                    </actions>

                                </wnd_activate_trigger>

```


Creating custom events

In addition to the standard events listed in [Generating database views](#), it is possible to create custom events to track application-specific events such as:

- Access to confidential data
- Attempted access to application features for which user is not authorized to use
- Access to application outside office hours

Custom events are created as a list of event code and display text pairs. They can be created by an Administrator through AccessAdmin as follows:

- Go to *System Policies >> AccessAudit Policies*.
- Add each pair of event code and display text to "List of custom audit event codes and their corresponding display names". Each event is entered as **<Event Code>,<Display Text>** where event code is a hexadecimal code in the range 0x43015000 to 0x43015FFF, inclusive. For example, "0x43015001,Access to confidential data".
- Using AccessStudio, create an AccessProfile that tracks the event and submits an audit log with that event code. See the **Generating a custom audit log section** of the AccessStudio Guide for details.

PART IV: USAGE AND RECOVERY WORKFLOWS

Part IV: Usage and Recovery Workflows

Use this part of the guide to learn more about managing workflows according to your organization's preferred desktop configuration, including workflows for recovery purposes. Refer to the following chapters:

- [Usage Workflows](#), which provides instructions on managing the desktop configurations for personal, shared, private, and roaming desktops.
- [Recovery Workflows](#), which contains instructions on handling user, computer, and server issues (e.g, data loss, system crashes, etc.).

Usage Workflows

The latest version of Encentuate IAM Enterprise supports two main usage configurations: personal workstations and shared workstations.

The personal workstation configuration is used in typical enterprise setups where users are assigned their own workstations. The recommended authentication factor for these configurations is the USB Key.

The shared workstation configuration is used in most healthcare organizations where doctors and nurses use any shared workstation that is available in the room. Such a usage scenario requires efficient switching of users on the shared workstation. Any other authentication factor besides the USB Key is recommended for the shared workstation configuration.

The chapter covers the following topics:

- [Managing workflows for personal workstations](#)
- [Managing workflows for shared workstations](#)

Managing workflows for personal workstations

The personal workstation configuration uses the USB Key as the authentication factor. Similar workflows and setup instructions apply if other authentication factors are used.

Setting up Encentuate IAM Enterprise (personal workstation)

Refer to this procedure to set up IAM enterprise in a personal workstation. You can also use the Setup Assistant wizard in AccessAdmin or IMS Configuration Utility. For more information on the Setup Assistant wizard, see the IAM Administrator Guide.

To set up Encentuate IAM Enterprise for a personal workstation:

- ❶ Install IMS Server and use the IMS Configuration Utility to set up the enterprise directory for validating Encentuate users.

If an authentication service is in a Windows domain, add it to the **DomainAuthenticatorGroup** authentication service group. For more information, see [Enterprise directory setup](#) of [IMS Server Setup](#).

- ❷ Set up the system policies through AccessAdmin, based on the recommended personal workstation values in the product specifications.
- ❸ Once personal workstation is chosen, machine policies are automatically created, based on the recommended personal workstation values in the product specifications.
- ❹ Set up user policies through AccessAdmin, by setting the default policy template based on the recommended personal workstation values in the product specifications. You can create multiple policy templates for different groups of users, provided that the policy templates are assigned correctly.
- ❺ (Optional) Write a logon script to auto-launch applications when users log on to AccessAgent. The logon script should be included in the policy template.
- ❻ (Optional) Write a logoff script to perform clean-up operations, if any, when users log off from AccessAgent. The logoff script should be included in the policy template.
- ❼ (Optional) Write lock or unlock scripts to perform actions before users lock the screen or after users unlock the screen. The lock and unlock scripts should be included in the policy template.
- ❽ (Optional) Set **pid_wallet_logoff_action_for_apps_default** and **pid_app_wallet_logoff_action** to perform auto-logoff or closing of applications when users log off from AccessAgent. Create AccessProfiles for all applications that require auto-logoff settings.
- ❾ Use AccessStudio to create and upload AccessProfiles for supported authentication services and applications through automatic logon and/or logoff.

Signing up from personal workstations

Users can sign up from EnGINA or from their desktop. Users are required to insert their USB Keys during sign up, but users can also initially sign up without USB Keys and register the USB Keys later when the Keys are available.

If a user signs up without a USB Key, the user can still log on to AccessAgent using an Encentuate password, provided that the authentication policy allows the logon process as an option.

To sign up from a personal workstation (with a USB Key):

- ❶ Insert an unregistered USB Key. The system displays a message, requesting to confirm if the user has already signed up.
- ❷ Click **Sign up**.
- ❸ Enter a unique user name.



The user name must not exceed 20 characters.

- ❹ Enter an Encentuate password, which will also be used as the USB Key password.
- ❺ Choose a secret question and provide the matching answer to the secret question.
- ❻ If the USB Key has not yet been inserted, AccessAgent displays a prompt to insert the USB Key.
- ❼ The system logs on the user to AccessAgent after completing the sign up process.

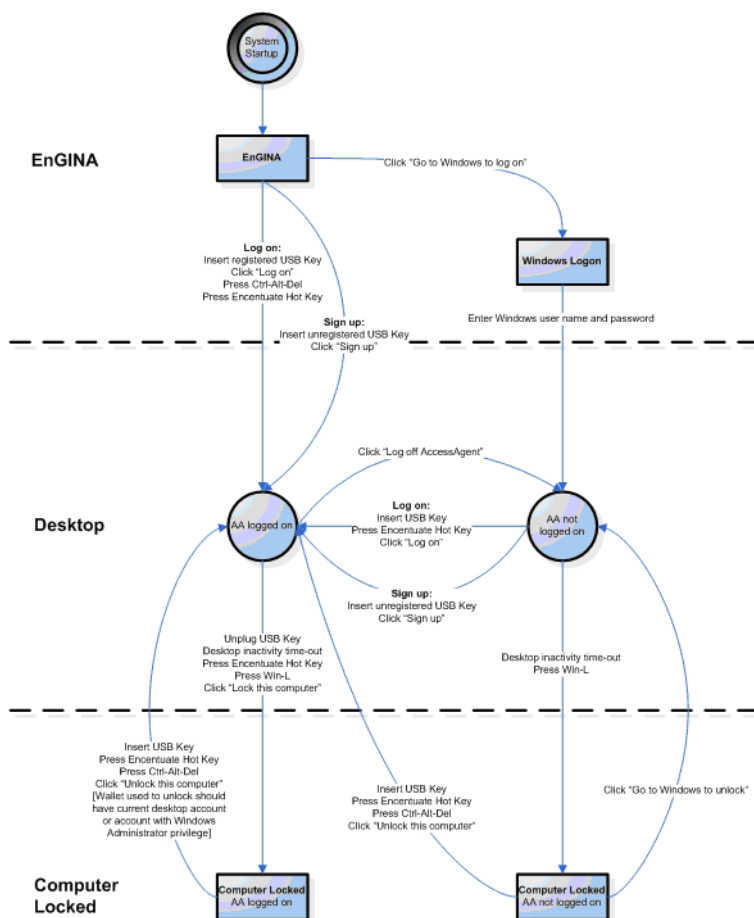
To register a USB Key (for users who have signed up without UBS Keys):

- ❶ Insert the unregistered USB Key. The system displays a message, requesting to confirm if the user has already signed up. Click **Yes**.
- ❷ Enter the Encentuate user name and password.
- ❸ Enter the authorization code provided by Helpdesk (only applicable if the authorization code is set on **pid_second_factor_registration_option**).
- ❹ The system logs on the user to AccessAgent after completing the registration process.

Personal workstation workflow

The personal workstation is configured to display the EnGINA screen upon start up. Refer to this topic to understand the product's behavior when using the EnGINA screen.

If users prefer to log on from Microsoft GINA, and in effect log on to both Windows and AccessAgent, both the ActiveDirectory password synchronization and the Encentuate Network Provider must be turned on. See Step 2 of 4 of Configuring the Active Directory section, IMS Configuration Utility in the Administrator Guide; and [Setup time only options](#) table, Installing AccessAgent in this Guide for details.



Personal workstation workflow

Personal workstation logon

- The user logs on from EnGINA.
- The user inserts USB Key to log on or presses **Ctrl+Alt+Del** to log on without a USB Key.
- The user's AccessAgent logon script, if any, is then executed.

Personal workstation lock

- The user removes the USB Key to lock the computer.
- AccessAgent automatically locks the computer after a configurable period of inactivity (**pid_desktop_inactivity_mins**).
- After locking the computer, an AccessAgent lock script, if any, is then executed.

Personal workstation unlock

- The user inserts the USB Key or presses **Ctrl+Alt+Del** to unlock the computer. The user is allowed to unlock the computer based on the settings in **pid_unlock_option**.
- After unlocking the computer, an AccessAgent unlock script, if any, is then executed.



*If transparent screen lock is enabled using the **pid_lock_option**, the unlock script will not be executed.*

Personal workstation logoff

- The user logs off from AccessAgent by right-clicking the AccessAgent icon and choosing the **Log off AccessAgent** option.
- During logoff, AccessAgent performs auto-logoff or closes applications depending on the policies **pid_wallet_logoff_action_for_apps_default** and **pid_app_wallet_logoff_action**.
- The user's AccessAgent logoff script, if any, is then executed.
- If the user logs off from Windows (e.g., clicking the **Log Off** option in the Windows Start Menu), AccessAgent logs off the user on a best-effort basis, within the logoff time-out provided by Windows. Since Windows will notify all applications to terminate, some may terminate before AccessAgent attempts to perform auto-logoff on the applications.

Managing workflows for shared workstations

In a working environment, such as in a hospital, doctors and nurses need to share computers. They usually move from one workstation to another for their work. This results in frequent **Switch User** tasks for each workstation. It's ideal that the switching of users should be fast and easy so that precious time can be saved.



These schemes do not make use of the Windows XP Fast User Switching feature.

Encentuate IAM Enterprise supports fast user switching through any of the following schemes:

■ **Fast User Switching through Shared Desktop**

Shared Desktops allow multiple users to use one (1) generic Windows desktop in a workstation. Since each user does not need to log on to Windows, the switching of users is quicker. However, after switching from User A to User B, the application contexts of User A will be lost. If User A returns later and switches the workstation back to User A's account, the user must re-launch the applications. For the scheme, AccessProfiles must be created to automatically log off enterprise applications when user switching occurs.

■ **Fast User Switching through Private Desktop**

Private Desktops allow multiple users to have their own Windows desktops in a workstation. The scheme uses the Local User Session Management feature of AccessAgent, which allows users to retain the existing user's desktop session during switching of users. When a User A returns to the workstation to unlock it, AccessAgent switches to User A's earlier desktop session, allowing User A to resume the previously incomplete or interrupted work. However, an existing desktop be logged off if the workstation runs out of resources (e.g., memory) to accept a new user logon. If the user logs on at another workstation, the user still needs to re-launch the applications.

■ **Fast User Switching through Roaming Desktop**

Roaming Desktops allow users' Windows desktops to "roam" to their points of access, from workstation to workstation. With roaming sessions, a user can disconnect from the current desktop or application session at a client, log on to another client, and continue the desktop or application session at a new client. The scheme requires the use of Terminal Server or Citrix, which is usually more costly to deploy.

When selecting which shared desktop scheme to deploy, consider the following details:

- Customer requirements
- Customer budget
- Limitations of each scheme
- Supported applications
- Authentication factors
- Workstation memory and speed

Setting workflows for shared desktops

For simplicity purposes, RFID is used as the authentication factor in the shared workstation with shared desktop example configuration. Similar workflows and setup instructions apply if other authentication factors are used.

Setting up Encentuate IAM Enterprise (shared desktop)

Refer to this procedure to set up IAM enterprise in a shared desktop. You can also use the Setup Assistant wizard in AccessAdmin or IMS Configuration Utility. For more information on the Setup Assistant wizard, see the IAM Administrator Guide.

To set up Encentuate IAM Enterprise for a shared desktop:

- ❶ Install IMS Server and use the IMS Configuration Utility to set up the enterprise directory for validating Encentuate users. If an authentication service is in a Windows domain, add it to the **DomainAuthenticatorGroup** authentication service group. For more information, see [Enterprise directory setup](#) of [IMS Server Setup](#).
- ❷ Set up the system policies through AccessAdmin, based on the recommended shared workstation values in the product specifications.
- ❸ Set up the machine policies through AccessAdmin, based on the recommended shared workstation values in the product specifications.
- ❹ Set up user policies through AccessAdmin, by setting the default policy template based on the recommended shared workstation values in the product specifications. You can create multiple policy templates for different groups of users, provided that the policy templates are assigned correctly.
- ❺ (Optional) Write a logon script to auto-launch applications when users log on to AccessAgent. The logon script should be included in the policy template.
- ❻ (Optional) Write a logoff script to perform clean-up operations, if any, when users log off from AccessAgent. The logoff script should be included in the policy template.
- ❼ (Optional) Write lock or unlock scripts to perform actions before users lock the screen or after users unlock the screen. The lock and unlock scripts should be included in the policy template.
- ❽ (Optional) Set **pid_wallet_logoff_action_for_apps_default** and **pid_app_wallet_logoff_action** to perform auto-logoff or closing of applications when users log off from AccessAgent. Create AccessProfiles for all applications that require auto-logoff settings.
- ❾ Use AccessStudio to create and upload AccessProfiles for supported authentication services and applications through automatic logon and/or logoff.

Signing up for shared desktops

Users can sign up from EnGINA, from their desktop, or from a locked computer. Users are required to tap their RFID cards during sign up, but can also initially sign up without RFID cards and register the RFID cards later when the cards are available.

If a user signs up without an RFID card, the user can still log on to AccessAgent using an Encentuate password, provided that the authentication policy allows the logon process as an option.

To sign up from a shared desktop:

- 1 Tap an unregistered RFID card on the RFID reader. The system displays a message, requesting to confirm if the user has already signed up.
- 2 Click **Sign up**.
- 3 Enter a unique user name.



The user name must not exceed 20 characters.

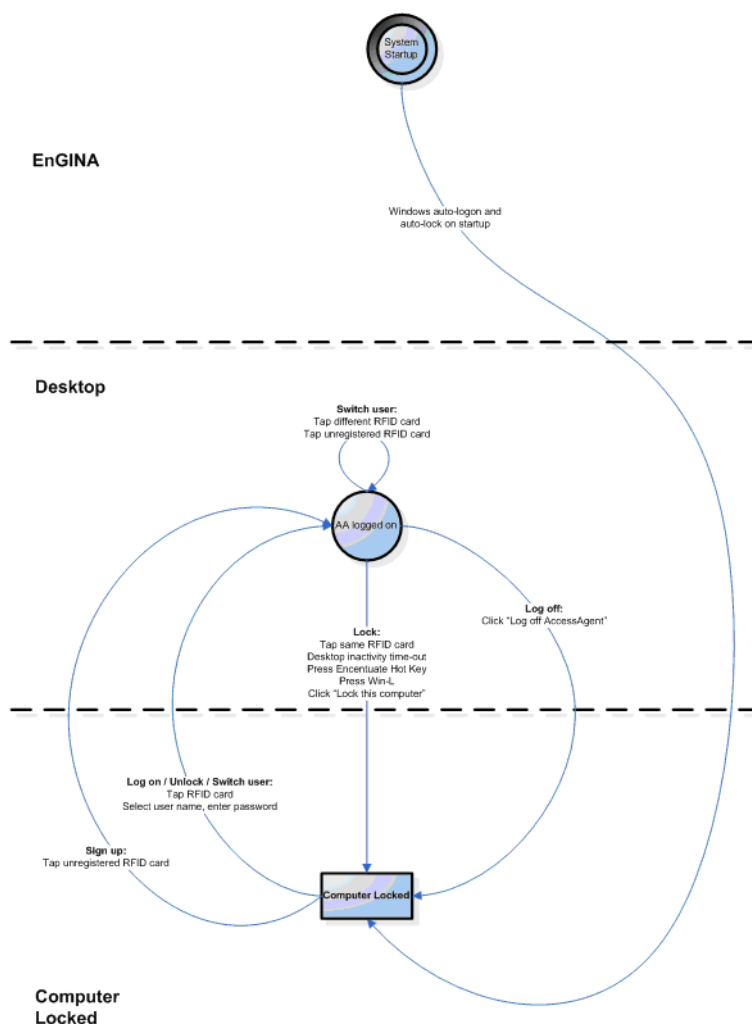
- 4 Enter an Encentuate password, if Active Directory password synchronization is disabled.
- 5 Choose a secret question and provide the matching answer to the secret question.
- 6 If the RFID card has not yet been tapped by the user, AccessAgent displays a prompt to tap the RFID card.
- 7 The system logs on the user to AccessAgent after completing the sign up process.

To register an RFID card (for users who have signed up without RFID cards):

- 1 Insert the unregistered RFID card. The system displays a message, requesting to confirm if the user has already signed up. Click **Yes**.
- 2 Enter the Encentuate user name and password.
- 3 Enter the authorization code provided by Helpdesk (only applicable if the authorization code is set on **pid_second_factor_registration_option**).
- 4 The system logs on the user to AccessAgent after completing the registration process.

Shared desktop workflow

The shared desktop is configured to log on automatically to a generic Windows account upon startup. The computer is locked when the Windows login is completed. Refer to the topic to understand the product's behavior when using a shared desktop.



Shared desktop workflow

Shared desktop logon

- The user logs on from the locked computer screen.
- The user taps the RFID card to log on or presses **Ctrl+Alt+Del** to log on without a RFID card. For users logging on with RFID cards, users may not need to enter their Encenulate passwords after logging on to other computers with the same RFID and password some time during the day (applicable only if settings on `pid_rfid_only_logon_enabled` and `pid_rfid_only_logon_timeout_mins` allow users to do so).
- The user's AccessAgent logon script, if any, is then executed.

Shared desktop lock

- The user taps the RFID card to lock the computer.
- AccessAgent automatically locks the computer after a configurable period of inactivity (**pid_desktop_inactivity_mins**).
- After locking the computer, an AccessAgent lock script, if any, is then executed.

Shared desktop unlock

- The user taps the RFID card to unlock the computer. The user is allowed to unlock the computer based on the settings in **pid_unlock_option**.
- The computer unlocks immediately upon RFID tap. After the period, user has to supply the Encentuate password to unlock the computer unless RFID-only logon is enabled. The user may not need to enter their Encentuate password after logging on to other computers with the same RFID and password some time during the day (applicable only if settings on **pid_rfid_only_logon_enabled** and **pid_rfid_only_logon_timeout_mins** allow users to do so).
- After unlocking the computer, an AccessAgent unlock script, if any, is then executed.



*If transparent screen lock is enabled using the **pid_lock_option**, the unlock script will not be executed.*

Shared desktop switch user

- Another user taps the RFID card to switching to another user, either from the desktop or from the locked computer screen.
- After the new user supplies a valid Encentuate password, AccessAgent unlocks the computer (if locked), log off the previous user, and then log on to the new user's Wallet. The users may not need to enter their Encentuate passwords after logging on to other computers with the same RFIDs and passwords some time during the day (applicable only if settings on **pid_rfid_only_logon_enabled** and **pid_rfid_only_logon_timeout_mins** allow users to do so).
- For a successful user switch scenario, the current user's running applications are automatically logged off. If AccessProfiles cannot be written to successfully log off an application (e.g., actions that require the application's user interface to be visible will not be possible), it will be terminated during user switching.

Shared desktop logoff

- The user logs off from AccessAgent by right-clicking the AccessAgent icon and choosing the **Log off AccessAgent** option.

- Logging off from the Wallet occurs when a different user tries to log on (see [Shared desktop switch user](#)).
- During logoff, AccessAgent performs auto-logoff or closes applications depending on the policies `pid_wallet_logoff_action_for_apps_default` and `pid_app_wallet_logoff_action`.
- If the logoff occurs behind a locked screen (e.g., during switch user), AccessAgent logs off the current user on a best-effort basis, since actions that require the application's user interface to be visible is not possible.
- The user's AccessAgent logoff script, if any, is then executed. If the logoff happens behind a locked screen (e.g., during switch user), the logoff script may not fully execute if requires any user interaction.
- If the user logs off from Windows (e.g., clicking the **Log Off** option in the Windows Start Menu), AccessAgent logs off the user on a best-effort basis, within the logoff time-out provided by Windows. Since Windows will notify all applications to terminate, some may terminate before AccessAgent attempts to perform auto-logoff on the applications.

Setting workflows for private desktops

The scheme uses the Local User Session Management feature of AccessAgent, which uses an Encentuate IAM Enterprise component called Encentuate Desktop Manager to manage concurrent user desktops on a single workstation.

Since logging on from the EnGINA welcome screen is not supported by Local User Session Management, workstations must be configured to automatically log on to a generic Windows account upon start up, and then lock the computer.



The generic Windows account must not be a registered Encentuate user. It is recommended to use a local machine user account.

All users must log on to the workstation from the locked screen. At any time, the screen should display the EnGINA locked screen or the currently visible desktop. There can be several invisible desktops that can be unlocked from the locked screen, or users can choose not to set invisible desktops.

The following Wallet authentication options are currently supported:

- Password
- RFID+Password
- ARFID+Password
- Fingerprint



Fingerprint authentication requires IMS Server 3.2.0.6 or a higher version.

If users log on to Windows sessions using their own Active Directory credentials, the Local User Session Management system must synchronize the Active Directory password and Encentuate password.

However, in some deployments, not all users may have Active Directory accounts. In the case, set up Local User Session Management to use a pool of computer accounts (either a Local machine or Active Directory account) to create the user desktop, and there would be no need to synchronize the Encentuate password and the Active Directory password.



Turning on Encentuate password aging will work only if the user logs in to AccessAgent before the Active Directory password expires and if the user changes the Encentuate password when the Encentuate password expires. See [Recommended settings](#) for details.

For simplicity purposes, the RFID is the authentication factor in the example of a shared workstation with a private desktop configuration. Similar workflows and setup instructions apply if other authentication factors are used.

Setting up Encentuate IAM Enterprise (private desktops)

Refer to this procedure to set up IAM enterprise in a private desktop. You can also use the Setup Assistant wizard in AccessAdmin or IMS Configuration Utility. For more information on the Setup Assistant wizard, see the IAM Administrator Guide.

To set up Encentuate IAM Enterprise for a private desktop:

- ❶ Install IMS Server and use the IMS Configuration Utility to set up the enterprise directory for validating Encentuate users. If an authentication service is in a Windows domain, add it to the **DomainAuthenticatorGroup** authentication service group. For more information, see [Enterprise directory setup](#) of [IMS Server Setup](#).

- ② Set up the system policies, based on the recommended shared workstation values in the product specifications. Read the Notes section of each policy to know which policy may not be supported when Local User Session Management is enabled (e.g., **pid_lusm_sessions_max** > 1).
- ③ Using AccessAdmin, set up the machine perform auto-admin logons. (**pid_microsoft_auto_logon_enabled**, **pid_microsoft_auto_logon_acct**).

AccessAgent is logged off if you are using an auto-admin account in a private desktop scenario.

- ④ Using AccessAdmin, set the machine policy (**pid_lusm_sessions_max**) that controls the number of concurrent user sessions (private desktops) supported on each workstation. The value must be greater than 1, which enables Local User Session Management.



You must modify the policy before AccessAgent is installed. If you modify the policy after AccessAgent is installed, the Log Off, Shut Down buttons, including the Windows hot keys may be disabled for the first user logging on. In addition, the buttons and Windows hot keys may remain disabled after AccessAgent is uninstalled.

- ⑤ Set up machine policies through AccessAdmin, based on the recommended shared workstation values in the product specifications. Read the Notes section of each policy to know which policy may not be supported when Local User Session Management is enabled (e.g., **pid_lusm_sessions_max** > 1).
- ⑥ (Optional) Modify the other policies with prefix **pid_lusm** according to requirements. Include the list of single instance applications (e.g., applications that cannot run on multiple simultaneous instances on a computer) in the **pid_lusm_sia_list**.
- ⑦ If generic accounts are used for creating user desktops, ensure that **pid_lusm_generic_accounts_enabled** is enabled and that the **pid_lusm_generic_accounts_list** contains the credentials of the generic accounts, which should be available on Active Directory or on individual machines (can be created using a script).

These generic accounts must have the **password never expires** attribute set. Note that the account passwords are entered clearly into the system registry and that these passwords are obscured by AccessAgent after machine startup. It is recommended to prepare the packaged **DeploymentOptions.reg** file with AccessAgent installers by exporting the system registry that contains the obscured passwords.



The auto-admin Windows logon account cannot be used as one of the generic accounts.

- ⑧ Set up user policies through AccessAdmin, by setting the default policy template based on the recommended shared workstation values.

Read the Notes section to know which policy may not be supported when Local User Session Management is enabled (e.g., **pid_lusm_sessions_max** > 1). You can create multiple policy templates for different groups of users, provided that the policy templates are assigned correctly.

- 9 (Optional) Write a logon script to auto-launch applications when users log on to AccessAgent. The logon script should be included in the policy template.
- 10 (Optional) Write a logoff script to perform clean-up operations, if any, when users log off from AccessAgent. The logoff script should be included in the policy template.
- 11 (Optional) Write lock or unlock scripts to perform actions before users lock the screen or after users unlock the screen. The lock and unlock scripts should be included in the policy template.
- 12 (Optional) Set **pid_wallet_logoff_action_for_apps_default** and **pid_app_wallet_logoff_action** to perform auto-logoff or closing of applications when users log off from AccessAgent. Create AccessProfiles for all applications that require auto-logoff settings.
- 13 Use AccessStudio to create and upload AccessProfiles for supported authentication services and applications through automatic logon and/or logoff.

Signing up for private desktops

Users can sign up from a locked computer. Users can tap their RFID cards during sign up, but users can also initially sign up without RFID cards and register the RFID cards later when the cards are available.

If a user signs up without an RFID card, the user can still log on to AccessAgent using an Encentuate password, provided that the authentication policy allows the logon process as an option.

To sign up from a private desktop:

- 1 Tap an unregistered RFID card on the RFID reader. The system displays a message, requesting to confirm if the user has already signed up.
- 2 Click **Sign up**.
- 3 Enter a unique user name.



The user name must not exceed 20 characters.

- 4 Enter an Encentuate password, if Active Directory password synchronization is disabled.

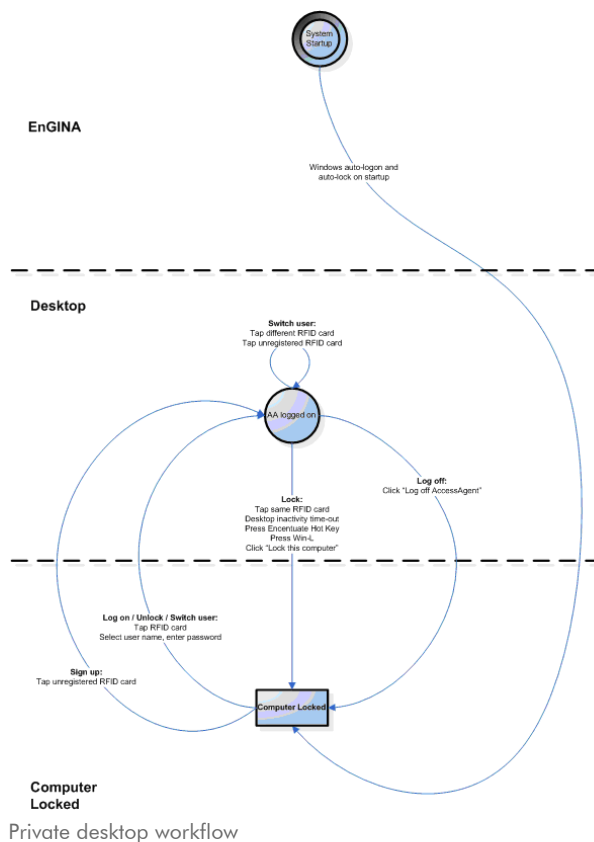
- 5 Choose a secret question and provide the answer to the secret question.
- 6 If the RFID card has not yet been tapped by the user, AccessAgent will display a prompt to tap the RFID card.
- 7 The user logs on to AccessAgent after completing the sign up process.

To register an RFID card (for users signed up without RFID cards):

- 1 Insert the unregistered RFID card. The system displays a message, requesting to confirm if the user has already signed up. Click **Yes**.
- 2 Enter the Encentuate user name and password.
- 3 Enter the authorization code provided by Helpdesk (only applicable if the authorization code is set on **pid_second_factor_registration_option**).
- 4 The user logs on to AccessAgent after completing the registration process.

Private desktop workflow

The private desktop is configured to log on automatically to a generic Windows account upon startup. The computer is locked when the Windows login is completed. Refer to this topic to understand the product's behavior when using a private desktop.



Private desktop logon

A user logs on to the workstation if the user does not have an existing invisible desktop running in the workstation (e.g., the user name is not shown on the locked screen, which lists the currently logged-on users).

- The user logs on from the locked computer screen.
- The user taps the RFID card to log on or clicks on **My logon user name is not in the list** to log on without an RFID card.
- To log on to a local Administrator account, use the convention `.\username` (e.g., if **Administrator** is the Administrator account, the user name would be `.\Administrator`).
- AccessAgent is logged off if you are using an auto-admin account in a private desktop scenario.
- If the user will access an RDP session with an auto-admin logon account, the remote user should log over the auto-admin session. The user will not be logged on to AccessAgent since the auto-admin session is using a local machine account, and AccessAgent logon is not supported.
- If the user will access an RDP with an admin account that is not the auto-admin logon account, the current session be logged off before the new session can start and allow a remote user to log on as an admin user. All running user desktops must be logged off. The user will then be logged on to AccessAgent.
- If the workstation does not have enough memory to create a new desktop or if the maximum number of concurrent sessions have been exceeded, AccessAgent may either block the new user from logging on, or automatically log off an existing invisible desktop (depending on the settings in `pid_lusm_session_replacement_option`).
- The user's AccessAgent logon script, if any, is then executed.
- If a single instance application is launched, an earlier instance run by another user may be logged off or closed (depending on the settings in `pid_lusm_sia_list` and `pid_lusm_sia_launch_option`).

Private desktop lock

- The user taps the RFID card to lock the computer.
- The user can also right-click AccessAgent and select **Lock the computer**, or press **Ctrl+Alt+Del** to activate the Windows Security dialog and select **Lock the computer**.
- If the user accessed an RDP session with an auto-admin logon account, disconnecting the RDP session displays the locked screen window. All user sessions are still connected.

- If the user accessed an RDP with an admin account that is not the auto-admin logon account, disconnecting the RDP session displays the locked screen window and automatically logs on again using auto-admin logon account.
- AccessAgent automatically locks the computer after a configurable period of inactivity (**pid_desktop_inactivity_mins**).
- After locking the computer, an AccessAgent lock script, if any, is then executed.

Private desktop unlock

A user can unlock a workstation if the user does not have an existing invisible desktop running in the workstation (such as, the user name is not shown on the locked screen, which lists the currently logged-on users).

- The user taps the RFID card to unlock the computer. The computer unlocks immediately after RFID tap if the user returns within a configurable period (**pid_rfid_only_unlock_timeout_secs**). After the period, user has to enter the Encuentra password to unlock the computer.
- The user can also unlock by selecting the user name from the list of currently logged-on users, and entering the user's password. Then, the user will need tap the RFID card.
- After unlocking, the user's existing invisible desktop becomes visible.
- After unlocking the computer, an AccessAgent unlock script, if any, is then executed.
- If the user had launched a single instance application before locking the workstation, the user may be logged off or closed (depends on settings in **pid_lusm_sia_list** and **pid_lusm_sia_launch_option**) while away from the workstation.

Configure AccessAgent to display the list of terminated single instance applications (depends on settings in **pid_lusm_sia_closed_apps_display_enabled**).

- For the RFID-only unlock feature, the timeout for each user is maintained separately. For example, if the RFID-only unlock time-out is five (5) minutes (**pid_rfid_only_unlock_timeout_secs**):
 - User A locks the screen at 12:00pm.
 - User B logs on at 12:02pm and locks it at 12:04pm.
 - User A unlocks the session at 12:06pm. User A enters the password after more than five (5) minutes have elapsed for the locked session. User A locks the screen at 12:07pm.
 - User B unlocks the session at 12:08pm. User B can unlock it without entering a password since four (4) minutes have elapsed for the locked session.

Private desktop switch user

From a locked screen:

- The user taps the RFID card to switch to the user's desktop by logging on (if the user has no existing invisible session) or by unlocking (if the user has an existing invisible session).
- If the workstation does not have enough memory to create a new desktop or has exceeded the maximum number of concurrent sessions, AccessAgent may either block the new user from logging on, or automatically log off an existing invisible desktop (depends on settings in `pid_lusm_session_replacement_option`).

From a visible desktop:

- The user taps the RFID card to switch to the user's existing invisible desktop or to log on to a new desktop. Whether the current desktop will be logged off or not depends on the settings in `pid_rfid_tap_different_action`.
- If the workstation does not have enough memory to create a new desktop or has exceeded the maximum number of concurrent sessions, AccessAgent may either block the new user from logging on, or automatically log off an existing invisible desktop (depends on settings in `pid_lusm_session_replacement_option`).

Private desktop logoff

- The user logs off from AccessAgent by right-clicking the AccessAgent icon and choosing the **Log off AccessAgent** option, or by pressing **Ctrl+Alt+Del** to activate the Encentuate Windows Security dialog box and selecting **Log off**.
- If the workstation does not have enough memory to create a new desktop, the previous user is logged off from the Wallet and desktop during user switch or when a different user logs on.
- When the machine is shut down, all users' sessions will be logged off.
- During logoff, AccessAgent performs auto-logoff or closes applications depending on the policies `pid_wallet_logoff_action_for_apps_default` and `pid_app_wallet_logoff_action`.
- If the logoff occurs behind a locked screen (e.g., during switch user), AccessAgent logs off the current user on a best-effort basis, since actions that require the application's user interface to be visible is not possible.
- To perform successful application logoff, set up AccessAgent to bring the desktop to be logged off at the front. A full screen status window is displayed so the current user cannot view another user's desktop during logoff. (based on settings in `pid_lusm_session_logoff_with_app_logoff_enabled`)

- The user's AccessAgent logoff script, if any, is then executed. If the logoff happens behind a locked screen (e.g., during switch user), the logoff script may not fully execute if it requires any user interaction.
- AccessAgent will also perform a Windows logoff for the user when logging off the user desktop (depends on settings in **pid_logoff_manual_action**).
- AccessAgent logs off the user on a best-effort basis, within the logoff timeouts specified in the **pid_lusm** policies. During the logoff process, AccessAgent attempts to auto-logoff the applications, then the Encentuate Desktop Manager terminates the user's other applications.

However, if AccessAgent cannot successfully auto-log off any applications within a specified timeout value (**pid_lusm_replace_app_close_timeout_secs** and **pid_lusm_logoff_app_close_timeout_secs**), the Encentuate Desktop Manager will still terminate all of the users' applications.

Similarly, if AccessAgent cannot execute the logoff script within a specified time-out value (**pid_lusm_replace_aa_logoff_timeout_secs** and **pid_lusm_logoff_aa_logoff_timeout_secs**), Encentuate Desktop Manager will terminate AccessAgent, and the logoff script not be executed.



Note that remote logoff of a workstation running private desktop can cause it to go into a bad state.

- After the user desktop is logged off, the locked screen is displayed, regardless of whether there are any more remaining invisible desktops.

Setting workflows for roaming desktops

For roaming sessions, the user's Windows desktop session can run on a remote Windows Terminal Server or Citrix server, so that the user can reconnect to the same Windows desktop session from any local workstation.

The solution is slightly different for the following:

- Windows Terminal Server (TS)
- Citrix MetaFrame Presentation Server

The use cases and workflows vary based on the configuration of local workstations. There are three (3) primary configurations for local workstations:

- Windows 2000 or Windows XP, with local AccessAgent
- Windows 2000 or Windows XP, without local AccessAgent
- Thin Client (Windows CE, Windows XPe), without local AccessAgent

The physical authentication factors used for logging on to AccessAgent from a remote desktop would also vary based on the configuration. Second factor authentication is managed using either of the following ways:

- The user logs on to local AccessAgent first, as AccessAgent can always verify the second factor.
- Map the local second factor device or port to the remote desktop over an RDP or ICA channel, so remote AccessAgent can receive the events from a physical device connected on the local workstation.
- Use second factor bypass to log on to the remote AccessAgent.
- Do not use second factor to log on to the remote AccessAgent.

Prerequisites for roaming desktops

Individual Active Directory (Windows) accounts for roaming

A user needs an Active Directory account to log on to the remote Windows desktop on TS through the RDP or ICA client.

Each user must log on to the TS using an individual Active Directory account for session persistence or roaming. It cannot be ensured that each user's session (e.g., AccessAgent session) persistence is successful, if a generic Active Directory account is used. An Encuentra user can switch the previous user's AccessAgent session on a generic Windows desktop.

Disconnect session for roaming

For TS or Citrix desktop, the disconnect and logoff concepts are different. If a user logs off from TS or Citrix, the remote Windows desktop disappears. However, if a user disconnects, the remote Windows desktop remains on the server.

Therefore, a user must disconnect instead of log off to use the roaming session. There are some exceptions for Windows 2003 Server. For more information, see the [Terminal Server issues and notes](#).

Publishing applications vs. full desktop

Accessing a published application from TS or Citrix is very different from accessing the full published desktop. For a Windows 2003 Server, both the desktop and application can be published and they can roam (such as, a user can reconnect back). However, there are restrictions on getting published applications to roam, with details described in [Terminal Server issues and notes](#). For Citrix, publishing applications are more common than publishing a desktop.

Terminal Server workflow for roaming desktops

This section describes the solution for roaming session on TS. For setup details, see [Installing roaming sessions on Terminal Server](#).

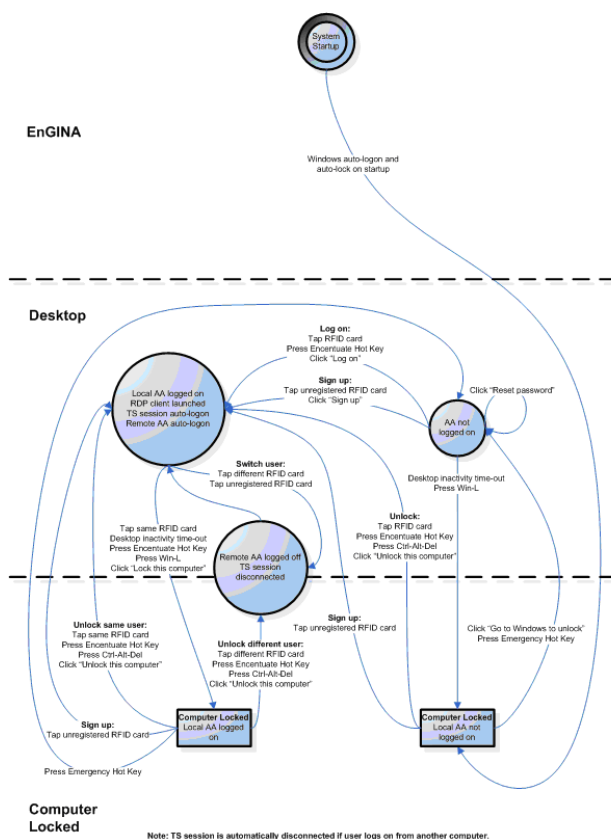
Terminal Server with local AccessAgent

The primary usage scenario is that the user logs on to local AccessAgent first, and then the user logs on to the remote AccessAgent on TS. There are two main usage patterns:

- The user runs all or most applications from the TS desktop.
- The user runs most of the applications from the local workstation, but uses the TS for some selected applications.

Context switching between local workstation and remote TS desktop applications can be challenging for users from a usability perspective, if some applications run on the local workstations and others run on the TS desktop. It is recommended that users run all or most applications from the TS desktop.

AccessAgent is installed on both the local workstation and TS. User applications are installed on the TS. The user logs on to the local AccessAgent, which automatically brings the user to the remote TS desktop session. The remote AccessAgent (running on TS) collaborates with the local AccessAgent (running on local workstation) and provides automatic sign-on to applications. The second factor verification is done by the local AccessAgent.



Roaming desktop workflow

All applications are assumed to be running on the TS. The shared workstation only needs to launch the RDP client when the user logs on to AccessAgent. Without loss of generality, the RFID card is used as a second factor. The workflow is similar for other second factors.

■ Log on to local AccessAgent

The logon may require a physical authentication factor, such as an RFID card, USB Key, active proximity badge, or a fingerprint.

The user logs on from EnGINA welcome screen, locked screen, or open desktop, based on the current behavior of AccessAgent.

The logon process must be automated to perform the following on a local workstation:

- Launch the RDP client.
- Enter the user's Active Directory user name, password, and domain in the RDP client. The RDP client will then log on to the TS desktop.



Auto-logon to TS by the RDP client only works if the "Use client-provided logon info" server setting is enabled and the "Always prompt for password" server setting is disabled. Otherwise, the user will see the remote GINA logon prompt. See [Installing roaming sessions on Terminal Server](#) in [Roaming Sessions](#).

- The remote desktop window is maximized to full screen mode.
- The AccessAgent running on the TS desktop interfaces with the local AccessAgent to get the Encuentate user name and password. AccessAgent then logs on to user's Wallet on the remote desktop.

Alternatively, if the customer disables the use of user credentials provided by the RDP client to log on to TS (see [Installing roaming sessions on Terminal Server](#) in [Roaming Sessions](#)), it is still possible to perform auto-logon for the RDP session as follows:

- Launch the RDP client.
- The remote desktop window is maximized to full screen mode.
- Remote Microsoft GINA appears within the RDP session.
- Local AccessAgent sends the user's Active Directory credentials over RDP channel.
- Remote AccessAgent (EnGINA module) receives the user's Active Directory credentials from the RDP channel, copies them into Microsoft GINA's logon prompt and clicks **OK** for automatic logon (depending on user's password entry option for Active Directory account).



The behavior of the system is the same as after logging on to EnGINA and Microsoft GINA. If there is no Active Directory account in the Wallet, AccessAgent auto-captures the entered credentials. If there are multiple Active Directory accounts in the Wallet, AccessAgent can prompt the user to select an account (if password entry options are set to Ask).

- The AccessAgent running on the TS desktop collaborates with the local AccessAgent to get the Encuentra user name and password. AccessAgent then logs on to user's Wallet on the remote desktop.

The user may have disconnected the TS session from a previous workstation without logging off from the remote desktop. The TS desktop session should persist. For such cases, the user would see the previous TS desktop running AccessAgent and other applications after the Active Directory user name and password have been verified through the RDP client.

The remote AccessAgent collaborates with the local AccessAgent to ensure that both the local and remote AccessAgent sessions belong to the same Encuentra user.

If the RDP client is launched through an AccessAgent logon script, ensure that the logon script can distinguish between local and remote AccessAgent sessions, since the same script is run by both local and remote AccessAgents.

If an RFID-only logon is enabled or fingerprint authentication is used at the local AccessAgent, the remote AccessAgent can only log on automatically to the same Wallet if Active Directory password synchronization is enabled.

■ The user locks the local workstation

A user can manually lock the local workstation or the workstation is automatically locked due to desktop inactivity. In either case, the TS desktop session should not be logged off to keep the session active. The local AccessAgent can disconnect the TS desktop before locking the workstation, so that the user can reconnect to the same TS desktop session from another computer.

A user policy (**pid_ts_lock_local_computer_action**) determines whether to disconnect the TS desktop session before locking the workstation. Personal desktop users may not want to disconnect their TS desktop session.

TS on Windows 2003 Server allows users to reconnect to both active and disconnected session from anywhere, provided the **Restrict each user to one session** server setting (or corresponding GPO policy) is enabled.

If user A logs into TS from machine T1, the existing active session at machine T2 will be disconnected with a warning. If the **Restrict each user to one session** setting is disabled, the user can only reconnect to disconnected sessions. Active sessions elsewhere will be left alone until they idle or timeout.

■ Disable locking of TS Desktop

The AccessAgent on the TS should disable locking the remote desktop, as the lock computer function is provided through local workstation. The **Lock this computer** option on the AccessAgent menu is automatically disabled.

It is recommended that the following should also be disabled:

- Screen saver leading to lock computer.
- Desktop inactivity time-out leading to lock computer.

■ The user logs off local AccessAgent

A user policy (`pid_ts_logoff_local_session_action`) determines whether to disconnect the TS desktop session during logging off AccessAgent.

■ The user unlocks the same local workstation

The user gets back to the same remote TS desktop session running AccessAgent and other applications.

■ The user logs on or unlocks from a different workstation

The user has already established a TS session from another workstation and the session was not logged off.

- The user unlocks or logs on to local AccessAgent.
- The RDP client is launched and logged to the TS desktop session.
- The remote AccessAgent collaborates with the local AccessAgent to ensure that both the local and remote AccessAgent sessions belong to the same Encentuate user. If the remote desktop session belongs to a different Encentuate user, the remote AccessAgent would log off from Wallet and re-logon to the local user's Wallet.



If RFID-only logon is enabled or fingerprint authentication is used at the local AccessAgent, the remote AccessAgent will only log on to the same Wallet automatically if Active Directory password synchronization is enabled.

- The user should see the previous TS desktop running AccessAgent and other applications.

Terminal Server without local AccessAgent

A user may connect to TS without logging on to local AccessAgent. This is possible if the local workstation does not have AccessAgent installed (e.g., home or Internet café), or if the user is connecting to TS from an open desktop and does not want to log on to local AccessAgent first. The workflows below are intended to handle this scenario.

■ The user launches RDP Client manually

The remote AccessAgent, having detected that there is no local AccessAgent session, will either display EnGINA or Microsoft GINA screen on the remote desktop. This is configurable using machine policy

pid_ts_engina_logon_no_local_session_enabled. The default is to display the EnGINA screen so user do not have to remember the Active Directory password.

- If the Microsoft GINA screen is configured to be displayed, the user should see a standard Windows logon screen. However, the user may have already entered the Active Directory user name, password, and domain in the local RDP client. In such a case, the user should be automatically logged on to the TS desktop.
- If the EnGINA screen is configured to be displayed, the user should see an EnGINA logon screen. In this case, even if the user has already entered the Active Directory user name, password and domain in the local RDP client, EnGINA will not use those information. The user has to either enter the Encentuate user name and password, or click **Go to Windows to log on** to bypass Encentuate logon.

■ Logging on to Remote AccessAgent

After logging on to the TS desktop, the remote AccessAgent attempts to communicate with a local AccessAgent but cannot find any local AccessAgent. Two configurations are possible:

- Encentuate password is the same as the Active Directory password.
- Encentuate password is not the same as the Active Directory password.

For the latter configuration, the machine policy **pid_ts_logon_prompt_enabled** determines the action taken by remote AccessAgent. There are two options:

- (Default) Prompt the user for an Encentuate user name and password. If the user's Wallet authentication policy requires to present a second factor, remote AccessAgent would request for an authorization code after verifying the Encentuate password (depends on the settings in **pid_ts_second_factor_bypass_option**).



This will result in a double logon. This problem can be resolved partially by encrypting the Encentuate password with the Active Directory password and storing it on IMS Server for the first time, then subsequently retrieving the encrypted Encentuate password, and then decrypting it with the Active Directory password. If the configuration is to use EnGINA logon screen but the user has chosen "Go to Windows to log on" to bypass Encentuate, remote AccessAgent would not prompt user to log on.

- Do not prompt user for Encentuate user name and password.



In this configuration, there is no remote AccessAgent session, and thus, no automatic sign-on to applications on the remote TS desktop. User may still manually log on to the remote AccessAgent by double-clicking the AccessAgent icon.

■ Remote AccessAgent session of reconnected TS session

The reconnected TS session may have an existing remote AccessAgent session running. Remote AccessAgent requires the user to log on before allowing him to continue with the session or to switch to a different Wallet. There are two possibilities:

- The user fails to log on to remote AccessAgent (e.g., wrong password). In such a case, the remote AccessAgent would log off the previous session, if any.
- The Encentuate user name is different from the one with the previous remote AccessAgent session. In such a case, the remote AccessAgent would trigger a switch user.

Terminal Server issues and notes

■ No support for TS on Windows 2000 Server

TS support is limited to Windows 2003 Server and above because:

- TS on Windows 2000 Server does not support **single session per user**, and roaming sessions would not work.
- TS on Windows 2000 Server does not support local COM port redirection or drive mapping. The Thin Client model would not work.
- TS on Windows 2000 Server does not support load-balancing and therefore it cannot scale to multiple TS servers for roaming sessions.

■ Limited number of users per TS

As the solution currently works for only one TS, the number of supported users will be limited per TS. The solution can potentially scale up to more users by deploying a TS farm on a Windows 2003 Server. This requires deploying/maintaining an identical set of applications on all member servers on the TS farm.

Though it is impractical to put all enterprise applications on a single TS, it is possible that different departments can have their own TS servers (or farms). If employees access only the applications of their department's TS server and not the others, then the system can support multiple silos of TS servers in the organization. For this case, customize each user's logon script (**pid_script_logon_code**) to launch the RDP client pointing to the correct TS (farm).

For customers with two or more TS silos, or customers with applications that do not run on TS, or have power users, set the logon script (**pid_script_logon_code**) to not auto-launch RDP upon local AccessAgent logon. In this case, the user can choose the appropriate TS to log on. These users need to toggle between local and remote desktops. Various RDP shortcuts can be created on the user's desktop for launching different groups of applications (e.g., finance, HR, etc.).

■ TS Desktop session per application instead of desktop

It is possible to support single-application RDP sessions by specifying a startup application in each RDP shortcut. These can also roam on a Windows 2003 Server. However, since users will not see seamless windows (see [Citrix](#)), there may be usability issues.

■ Reconnecting without disconnecting last session on Windows 2003 Server

The following behaviors have been observed when limiting each user to one active session using the **Restrict each user to one session** setting:

- To launch an RDP session at machine T1 with the same startup command (or none, for entire desktop) as an existing "active" session running on machine T2, the existing session at T2 will be disconnected with a warning, and reconnected at T1. The warning message at T1 says "The remote session was disconnected because another user has connected to the session."

It does not matter whether the RDP settings for color depth, screen size, etc. are different. TS will reconnect the session provided that the startup command is null or identical (case-insensitive).

However, it does matter that the startup commands are the same (textual case-insensitive string equality), even if they launch the same application. If an RDP client on T1 has a startup command **tsadmin.exe** and RDP client on T2 has startup command **tsadmin.exe 1234**, then two different sessions will be launched. Or if T2 has startup command **C:\windows\system32\tsadmin.exe**, then two different sessions will also be launched. But if one says **tsadmin.exe** and the other says **tsadmin.EXE**, the reconnection will happen.

- The **Restrict each user to one session** constraint does not restrict the user from launching multiple TS sessions using different startup commands. If the user has RDP shortcuts to Notepad, Word, and Internet Explorer on a TS, three different TS sessions can be launched. But the user cannot have two concurrent sessions with Notepad, unless the user varies the command line text - using **Notepad** on one and **Notepad.exe** on another.
- The **Restrict each user to one session** feature is not available on Windows 2000 Server.

■ Password encryption enabled

For older installations of Terminal Server, be sure to turn on password encryption so that clear-text passwords will not be sent over the RDP channel. By default, newer installations of Terminal Server already have password encryption enabled.

Citrix

This section describes the solution for roaming session on Citrix MetaFrame Presentation Server. For details on setup, see [Installing roaming sessions on Citrix](#).

Citrix with local AccessAgent

The primary usage scenario is that the user first logs on to local AccessAgent, and then the user logs on to the remote AccessAgent on Citrix.

There are two main usage patterns:

- The user runs all or most applications from the published Citrix server desktop.
- The user runs most of the applications from the local workstation, but uses the Citrix server for some selected published applications.

In a typical Citrix deployment, customers use published applications instead of a published desktop. When a user launches a published application from a Citrix program neighborhood, the local AccessAgent copies the user's Active Directory credentials in the ICA client dialog, which automatically logs on the user to the remote desktop.

The remote AccessAgent running on the remote desktop interfaces with the local AccessAgent to log on to the user's Wallet on the remote desktop and subsequently provides automatic sign-on to the published applications.

Most of the workflows are similar to AccessAgent with TS. The following sections only highlight the differences.

Summary of the main differences are:

Terminal Server	Citrix
RDP client is used.	ICA client is used, from Program Neighborhood or Web Interface.
Entire remote desktop is used. There is always one remote desktop (for one server).	Published applications are used. There can be multiple remote application sessions running on different servers.
Local AccessAgent launches RDP client automatically in full screen mode.	The user launches published applications as needed.
The user reconnects back to the same remote desktop.	The user reconnects back to individual published applications.

Terminal Server	Citrix
EnGINA is used by users to log on manually.	EnGINA is not used for logon.
Terminal server is used.	Citrix automatically supports multiple MetaFrame servers for load balancing. Different applications can be published on different servers and the mechanism of publishing applications is automated.

■ The user logs on to local AccessAgent

After logging on to the local AccessAgent, Citrix ICA clients are typically not launched automatically. When the user logs on to a specific published application on the Citrix server, the user launches the application from Citrix Program Neighborhood on the local workstation. The workflow is as follows:

- Local ICA client logon prompt is displayed.
- Local AccessAgent auto-fills user's Active Directory user name, password, and domain.
- ICA client logs on to the Citrix server.



*Auto-logon to Citrix server only works, if the **Use client-provided logon info** server setting is enabled and the **Always prompt for password** server setting is disabled. Otherwise, the user will see the remote Microsoft GINA logon prompt.*

- The remote AccessAgent running on the Citrix desktop collaborates with the local AccessAgent to get the Encuentate user name and password. It then logs on to user's Wallet on remote desktop.

The user may have disconnected a previous Citrix session with the same application without logging off from the remote desktop. The Citrix session with the application should be active. In such case, after verifying the Active Directory user name and password through the ICA client, the user would see the previous desktop session running AccessAgent and the same application.

However, the remote AccessAgent collaborates with the local AccessAgent to ensure that both the local and remote AccessAgent sessions belong to the same Encuentate user. If the local and remote AccessAgent sessions belong to two different Encuentate users, the remote AccessAgent would log off the previous user's Wallet and re-log on to the local user's Wallet.

The user may launch Internet Explorer and go to a URL instead of launching the local ICA client to use a published application. The behavior should be similar to what is described above.

If RFID-only logon is enabled or fingerprint authentication is used at the local AccessAgent, the remote AccessAgent can only log on automatically to the same Wallet if Active Directory password synchronization is enabled.

■ The user locks the local workstation

The user can manually lock the local workstation or the workstation is locked due to desktop inactivity. In either case, the local AccessAgent may disconnect the Citrix session, if any, before it locks the workstation. The user can then reconnect to the same Citrix application session from another computer.

A user policy (**pid_ts_lock_local_computer_action**) determines whether to disconnect the Citrix session before locking the workstation. Personal desktop users may not want to disconnect their Citrix session.

■ Disable locking the Citrix Desktop

The AccessAgent on Citrix should disable locking the remote desktop, as the lock computer function is provided through a local workstation. The **Lock this computer** option on the AccessAgent menu is automatically disabled.

It is recommended that the following should also be disabled:

- Screen saver leading to lock computer.
- Desktop inactivity time-out leading to lock computer.

■ The user logs off local AccessAgent

A user policy (**pid_ts_logoff_local_session_action**) determines whether to disconnect the Citrix session during AccessAgent logoff.

■ The user unlocks the same local workstation

The user needs to manually reconnect the Citrix applications on the local workstation after unlocking. Then, the user can resume the previous application sessions on the remote desktop.

■ The user logs on or unlocks from a different workstation

The user has already established one or more application sessions from other workstations and the sessions were disconnected.

- The user unlocks or logs on to local AccessAgent.
- The user may launch some published applications from the Citrix Program Neighborhood.
- Local ICA client logon prompt is displayed.

- Local AccessAgent auto-fills user's Active Directory user name, password and domain.
- ICA client logs on to the Citrix server.
- The remote AccessAgent collaborates with the local AccessAgent to ensure that both the local and remote AccessAgent sessions belong to the same Encentuate user.

If the remote AccessAgent session belongs to a different Encentuate user, the remote AccessAgent should log off from the Wallet and log on again to the local user's Wallet. If RFID-only logon is enabled or fingerprint authentication is used at the local AccessAgent, the remote AccessAgent will log on automatically to the same Wallet if Active Directory password synchronization is enabled.

- The user should see the previous session running AccessAgent and the application.

The user may launch Internet Explorer and go to a URL instead of launching the local ICA client to use a published application. The behavior should be similar to what is described above.

Citrix without local AccessAgent

A user may connect to Citrix without first logging on to local AccessAgent. This is possible if the local workstation does not have AccessAgent installed (e.g., home or Internet café), or if the user is connecting to Citrix from an open desktop and does not want to log on to local AccessAgent.

The only workflow intended to handle this scenario is "the user launches ICA Client manually".

The behavior is similar to the corresponding section to handle TS without local AccessAgent. The policy `pid_ts_engina_logon_no_local_session_enabled` should be set to `0` so that the Microsoft GINA screen is displayed, as the ICA client cannot handle pass-through or client-side logon.

Citrix issues and notes

■ Published applications in "seamless windows" mode

With published applications in **seamless windows** mode, users do not typically disconnect. When they click the **x** in the window, the application will close. There is no button on the application window to disconnect the session. The way to disconnect the session may not be obvious, depending on usage scenarios. If applications are closed instead of disconnected, the roaming session would be meaningless.

If the user is using the Web Interface with **seamless windows** mode, applications can be disconnected by clicking on the **Disconnect** button of the Web Interface page. Alternatively, the user can also right-click the Web Client, click **Open Connection Center**, select the appropriate Citrix server, and click **Disconnect**.

If the user is using the Program Neighborhood Agent with **seamless windows** mode, applications can be disconnected by right-clicking the Program Neighborhood Agent, and clicking **Disconnect**.

■ Published applications in "non-seamless windows" mode

With published application in **non-seamless windows** mode, users can simply click on the window **Close** button of the MetaFrame Presentation Server Client window to disconnect. However, there are problems with **non-seamless windows** mode:

- Applications appear disorganized compared to seamless windows; a user sees one window nested within another.
- It can get confusing if **session sharing** is enabled (such as, disconnecting one application will close a few windows and reconnecting one application will bring up a few windows).

■ Workspace control

For Citrix deployments using MetaFrame XP, MetaFrame Presentation Server 3/4 without NFuse, or MetaFrame Presentation Server 3/4 with NFuse but with **Workspace Control** feature disabled, if the user has an active session running, there is no option to reconnect to this session on another machine until the active session is disconnected (via timeout or admin-disconnect).

If set to **restrict each user to one session**, the user will not be connected. If set without the restriction, the user will receive a new session while the earlier session remains active.

In Citrix Presentation Server 3/4 deployments using NFuse with **Workspace Control** enabled, users can reconnect to active sessions running elsewhere. However, users must use NFuse to retrieve its Program Neighborhood, either via NFuse Web Interface, or via the Program Neighborhood Agent. Those using the regular Program Neighborhood client (which uses a locally-configured Program Neighborhood) will not access the **Workspace Control** feature.

■ Password encryption enabled

For older installations of Citrix Server, be sure to turn on password encryption so that clear-text passwords will not be sent over the ICA channel. By default, newer installations of Citrix Server already have password encryption enabled.

Recovery Workflows

Encentuate IAM Enterprise supports several recovery scenarios so that users can access their computers and applications even when operational problems are encountered. This chapter lists the various operational problems and their associated recovery workflows.

Note that the workflow may depend on whether IMS Server is accessible from AccessAgent (indicated as "online" or "offline").

The chapter covers the following topics:

- [Recovery workflows for user issues](#)
- [Recovery workflows for computer issues](#)
- [Recovery workflows for server issues](#)

Recovery workflows for user issues

Forgetting the Encentuate password (online)

Operational problem:

The user tries to log on to AccessAgent but has forgotten the Encentuate password (e.g., not using a USB Key).

Situational conditions (self-service password reset disabled):

- AccessAgent can contact the IMS Server.
- The user can contact Helpdesk.

Recovery workflow (self-service password reset disabled):

- ❶ The user clicks **Reset password** in AccessAgent.
- ❷ AccessAgent prompts the user to enter an authorization code, which is obtained from Helpdesk.
- ❸ The user supplies the authorization code and the secret answer (secret question will be displayed).
- ❹ The user is asked to specify a new Encentuate password.
- ❺ The user can now log on using the new Encentuate password.



Cached Wallets will still have locks that use the old password until user attempts to log on to them while the IMS Server is available. If the IMS Server is not available when the user tries to log on to a cached Wallet, the old password will only be accepted.

Situational conditions (self-service password reset enabled):

- AccessAgent can contact the IMS Server.

Recovery workflow (self-service password reset enabled):

- ❶ The user clicks on **Reset password** option of AccessAgent.
- ❷ AccessAgent prompts user to select his secret questions (previously specified) and provide the corresponding answers.
- ❸ The user is asked to specify a new Encentuate password.
- ❹ The user can now log on using the new Encentuate password.

Forgetting the Encentuate password (offline)

Operational problem:

- The user tries to log on to AccessAgent but has forgotten the Encentuate password (e.g., not using a USB Key).

Situational conditions:

- AccessAgent cannot contact the IMS Server.
- The computer has the user's cached Wallet.
- The user can contact Helpdesk.

Recovery workflow:

- ① The user clicks the **Reset password** option of AccessAgent.
- ② AccessAgent displays a request code and prompts the user to enter an authorization code, which is obtained from Helpdesk. To be issued an authorization code, the user needs to provide the request code. Helpdesk should select the appropriate validity period before issuing the authorization code.
- ③ The user supplies the authorization code and the secret answer (secret question will be displayed).
- ④ The user specifies a temporary password since the IMS Server is not available.
- ⑤ The user can log on (multiple times) to this computer only using the temporary password, until the authorization code expires.



Since the temporary password is only created on the user's current computer, the user must reset the password again when logging on to another computer.

Forgetting the USB Key password (online)

Operational problem:

- The user tries to log on to AccessAgent but has forgotten the USB Key password (such as, logging on with a USB Key).

Situational conditions:

- AccessAgent can contact the IMS Server.
- The user can contact Helpdesk.

Recovery workflow:

- ① The user contacts Helpdesk. Helpdesk will advise to reset the password without inserting the USB Key. The Administrators or Helpdesk users are the only users authorized to reset USB Key passwords.
- ② The user removes the USB Key and clicks **Reset password** option of AccessAgent.
- ③ AccessAgent prompts the user to enter an authorization code, which is obtained from Helpdesk. Helpdesk should select the appropriate validity period of validity before issuing the authorization code.
- ④ The user supplies the authorization code and the secret answer (secret question will be displayed).

- 5 The user is asked to specify a new Encentuate password.



The Encentuate passwords will no longer synchronize with the USB Key passwords even for normal users (such as, `pid_enc_pwd_is_usb_key_pwd_enabled` is `True`).

- 6 The user clicks **Log on** in AccessAgent.
- 7 The user supplies the Encentuate user name and password.
- 8 The user clicks **...but I do not have my Encentuate USB Key with me**.
- 9 The user supplies the authorization code previously obtained from Helpdesk.
- 10 The user can log on (multiple times) to this computer only using the temporary password, until the authorization code expires.
- 11 To log on to another computer, user clicks on **...but I do not have my Encentuate USB Key with me** again and supplies the same authorization code. The user can then log on (multiple times) to the second computer, without using USB Key, until the authorization code expires.
- 12 The user returns the USB Key to Helpdesk to be reset. Helpdesk revokes the USB Key through AccessAdmin, resets the USB Key, and returns it to the user.
- 13 The user inserts the newly reset USB Key. When asked by the system whether the user had already signed up, click **Yes**.
- 14 The user supplies the Encentuate user name and password.
- 15 The user supplies the authorization code previously obtained from Helpdesk.
- 16 The user is logged on to AccessAgent after completing the registration. The user can now log on to the USB Key with the new password.

Forgetting the USB Key password (offline)

Operational problem:

- The user tries to log on to AccessAgent but has forgotten the USB Key password (e.g., logging on with a USB Key).

Situational conditions:

- AccessAgent can contact the IMS Server.
- The computer has the user's cached Wallet.
- The user can contact Helpdesk.

Recovery workflow:

- ❶ The user contacts Helpdesk. Helpdesk will advise to reset the password without inserting the USB Key. The Administrators or Helpdesk users are the only users authorized to reset USB Key passwords.
- ❷ The user removes the USB Key and clicks **Reset password** option of AccessAgent.
- ❸ AccessAgent displays a request code and prompts user to enter an authorization code is obtained from Helpdesk. The user needs to provide the request code before Helpdesk can issue an authorization code. Helpdesk should select the appropriate validity period of validity before issuing the authorization code.
- ❹ The user supplies the authorization code and the secret answer (secret question will be displayed).
- ❺ The user is asked to specify a temporary password since IMS Server is not available.
- ❻ The user can log on (multiple times) to this computer only using the temporary password, until the authorization code expires.



Since the temporary password is only created on the user's current computer, the user must reset the password again when logging on to another computer.

- ❼ The user returns the USB Key to Helpdesk to be reset. Helpdesk revokes the USB Key through AccessAdmin, resets the USB Key, and returns it to the user. Helpdesk should also issue him with an authorization code through AccessAdmin.
- ❽ The user clicks the **Reset password** option of AccessAgent.
- ❾ The user supplies the authorization code previously obtained from Helpdesk and the secret answer (secret question will be displayed).
- ❿ The user is asked to specify a new Encentuate password.
- ⓫ The user inserts the newly reset USB Key. When asked by the system whether the user had already signed up, click **Yes**.
- ⓬ The user supplies the Encentuate user name and password.
- ⓭ The user supplies the authorization code previously obtained from Helpdesk.
- ⓮ The user is logged on to AccessAgent after completing the registration. The user can now log on to the USB Key with the new password.

Forgetting or losing the USB Key (online)

Operational problem:

- The user tries to log on to AccessAgent but has either forgotten to bring the USB Key, the USB Key is lost, or the USB Key is malfunctioning.

Situational conditions (self-service bypass of second factor disabled):

- AccessAgent can contact the IMS Server.
- The user can contact Helpdesk.

Recovery workflow (self-service bypass of second factor disabled):

- 1 The user clicks **Log on** in AccessAgent.
- 2 The user supplies the Encentuate user name and password.
- 3 The user clicks **...but I do not have my Encentuate USB Key with me** to bypass the use of the second factor.
- 4 AccessAgent prompts the user to enter an authorization code which is obtained from Helpdesk. Helpdesk should select the appropriate validity period of validity before issuing the authorization code. If the USB Key is lost or is malfunctioning, Helpdesk should revoke the USB Key through AccessAdmin.
- 5 The user can log on (multiple times) to this computer only, without using the USB Key, until the authorization code expires.
- 6 To log on to another computer, user clicks on **...but I do not have my Encentuate USB Key with me** again and supplies the same authorization code. The user can then log on (multiple times) to the second computer, without using USB Key, until the authorization code expires.
- 7 The user returns the USB Key to Helpdesk to be reset. Helpdesk revokes the USB Key through AccessAdmin, resets the USB Key, and returns it to the user.

Additional workflow for lost or malfunctioning USB Key (self-service bypass of second factor disabled):

- 8 Helpdesk issues the user with a new USB Key.
- 9 The user inserts the new USB Key. When asked by the system whether the user had already signed up, click **Yes**.
- 10 The user supplies the Encentuate user name and password.

- ⑪ The user supplies the authorization code previously obtained from Helpdesk.
- ⑫ The user is logged on to AccessAgent after completing the registration.

Situational conditions (self-service bypass of second factor enabled):

- AccessAgent can contact the IMS Server.

Recovery workflow (self-service bypass of second factor enabled):

- ① The user clicks **Log on** in AccessAgent.
- ② The user supplies the Encentuate user name and password.
- ③ The user clicks **...but I do not have my Encentuate USB Key with me** to bypass the use of the second factor.
- ④ AccessAgent prompts the user to select the appropriate secret question and secret answer combination.
- ⑤ The user can log on (multiple times) to this computer only, without using the USB Key, for one (1) day.
- ⑥ To log on to another computer, user clicks on **...but I do not have my Encentuate USB Key with me** again and answer the self-service questions. The user can then log on (multiple times) to the second computer, without using USB Key, for one day.

Additional workflow for lost or malfunctioning USB Key (self-service bypass of second factor enabled):

- ⑦ Helpdesk issues the user with a new USB Key.
- ⑧ The user inserts the new USB Key. When asked by the system whether the user had already signed up, click **Yes**.
- ⑨ The user supplies the Encentuate user name and password.
- ⑩ AccessAgent prompts the user to select the appropriate secret question and secret answer combination.
- ⑪ The user is logged on to AccessAgent after completing the registration.

Forgetting or losing the USB Key (offline)

Operational problem:

- The user tries to log on to AccessAgent but has either forgotten to bring the USB Key, the USB Key is lost, or the USB Key is malfunctioning.

Situational conditions:

- AccessAgent cannot contact the IMS Server.
- The computer has the user's cached Wallet.
- The user can contact Helpdesk.

Recovery workflow:

- 1 The user clicks **Log on** in AccessAgent.
- 2 The user supplies the Encentuate user name and password.
- 3 AccessAgent displays a request code and prompts the user to enter an authorization code, which is obtained from Helpdesk. The user needs to provide the request code so Helpdesk can issue an authorization code. Helpdesk should select the appropriate validity period of validity before issuing the authorization code. If the USB Key is lost or is malfunctioning, Helpdesk should revoke the USB Key through AccessAdmin.
- 4 The user supplies the authorization code and the answer (secret question will be displayed).
- 5 The user is asked to specify a temporary password since IMS Server is not available.
- 6 The user can log on (multiple times) to this computer only using the temporary password, until the authorization code expires.



Since the temporary password is only created on the user's current computer, the user must reset the password again when logging on to another computer.

Additional workflow for lost or malfunctioning USB Key:

- 7 Helpdesk issues the user with a new USB Key.
- 8 The user inserts the new USB Key. When asked by the system whether the user had already signed up, click **Yes**. The computer must be able to contact IMS Server.
- 9 The user supplies the Encentuate user name and password.

- ⑩ AccessAgent prompts the user to enter an authorization code, which is obtained from Helpdesk.
- ⑪ The user is logged on to AccessAgent after completing the registration.

Forgetting or losing the RFID card (online)

Operational problem:

- The user tries to log on to AccessAgent but has forgotten to bring the RFID card, or the RFID card is lost, or the RFID card is malfunctioning.

Situational conditions (self-service bypass of second factor disabled):

- AccessAgent can contact the IMS Server.
- The user can contact Helpdesk.

Recovery workflow (self-service bypass of second factor disabled):

- ① The user clicks **Log on** in AccessAgent.
- ② The user supplies the Encentuate user name and password.
- ③ User clicks **...but I do not have my RFID card with me** to bypass the use of second factor.
- ④ AccessAgent prompts the user to enter an authorization code, which is obtained from Helpdesk. Helpdesk should select the appropriate validity period of validity before issuing the authorization code. If the RFID card is lost or is malfunctioning, Helpdesk should revoke the RFID card through AccessAdmin.
- ⑤ The user can log on (multiple times) to this computer only, without using the RFID card, until the authorization code expires.
- ⑥ To log on to another computer, user clicks on **...but I do not have my RFID card with me** again and supply the same authorization code. The user can then log on (multiple times) to the second computer, without using RFID card, until the authorization code expires.

Additional workflow for lost or malfunctioning RFID card (self-service bypass of second factor disabled):

- ⑦ Helpdesk issues the user with a new RFID card.

- ⑧ The user taps the new RFID card. When asked by the system whether the user had already signed up, click **Yes**.
- ⑨ The user supplies the Encentuate user name and password.
- ⑩ The user supplies the authorization code previously obtained from Helpdesk.
- ⑪ The user is logged on to AccessAgent after completing the registration.

Situational conditions (self-service bypass of second factor enabled):

- AccessAgent can contact the IMS Server.

Recovery workflow (self-service bypass of second factor enabled):

- ① The user clicks **Log on** in AccessAgent.
- ② The user supplies the Encentuate user name and password.
- ③ The user clicks **...but I do not have my RFID card with me** to bypass the use of the second factor.
- ④ AccessAgent prompts the user to select the appropriate secret question and secret answer combination.
- ⑤ The user can log on (multiple times) to this computer only, without using the USB Key, for one (1) day.
- ⑥ To log on to another computer, user clicks on **...but I do not have my RFID card with me** again and answer the self-service questions. The user can then log on (multiple times) to the second computer, without using RFID, for one (1) day.

Additional workflow for lost or malfunctioning RFID card (self-service bypass of second factor enabled):

- ⑦ Helpdesk issues a new RFID card for the user.
- ⑧ The user taps the new RFID card. When asked whether the user had already signed up, click **Yes**.
- ⑨ The user supplies the Encentuate user name and password.
- ⑩ AccessAgent prompts the user to select the appropriate secret question and secret answer combination.
- ⑪ The user is logged on to AccessAgent after completing the registration.

Forgetting or losing the RFID card (offline)

Operational problem:

- The user tries to log on to AccessAgent but has either forgotten to bring the RFID card, the RFID card is lost, or the RFID card is malfunctioning.

Situational conditions:

- AccessAgent cannot contact the IMS Server.
- The computer has the user's cached Wallet.
- The user can contact Helpdesk.

Recovery workflow:

- ① The user clicks **Log on** in AccessAgent.
- ② The user supplies the Encentuate user name and password.
- ③ The user clicks **...but I do not have my RFID card with me** to bypass the use of the second factor.
- ③ AccessAgent displays a request code and prompts the user to enter an authorization code, which is obtained from Helpdesk. The user needs to provide the request code so Helpdesk can issue an authorization code. Helpdesk should select the appropriate validity period of validity before issuing the authorization code. If the RFID card is lost or is malfunctioning, Helpdesk should revoke the RFID card through AccessAdmin.
- ④ The user supplies the authorization code and the answer (secret question will be displayed).
- ⑤ The user specifies a temporary password since the IMS Server is not available.
- ⑥ The user can log on (multiple times) to this computer only using the temporary password, until the authorization code expires.



Since the temporary password is only created on the user's current computer, the user must reset the password again when logging on to another computer.

Additional workflow for lost or malfunctioning RFID card:

- ⑦ Helpdesk issues the user with a new RFID card.
- ⑧ The user taps the new RFID card. When asked whether the user had already signed up, click **Yes**. The computer must be able to contact IMS Server.

- 9 The user supplies the Encentuate user name and password.
- 10 AccessAgent prompts the user to enter an authorization code, which is obtained from Helpdesk.
- 11 The user is logged on to AccessAgent after completing the registration.

Recovery workflows for computer issues

Cannot unlock the computer successfully (shared workstation)

Operational problem:

- The user tries to log on to AccessAgent and unlock the computer but is unsuccessful. This may be because there is no cached Wallet on the computer and the computer cannot contact the IMS Server.

Situational conditions:

- The computer is a shared workstation with **Emergency Hot Key** enabled.

Recovery workflow:

- 1 The user presses the **Emergency Hot Key** sequence.
- 2 The computer is now unlocked.



All users logged on to AccessAgent must be logged off.

AccessAgent is not installed

Operational Problem:

- The user wants to log on to some enterprise applications, has forgotten the application passwords and AccessAgent is not installed on the computer.

Situational conditions:

- The computer can access AccessAssistant.
- AccessAssistant is enabled for the user (`pid_accessanywhere_enabled`).

Recovery workflow:

- ❶ The user launches the Web browser to access AccessAssistant.
- ❷ The user supplies the Encentuate user name and password.
- ❸ If second factor authentication is required (`pid_accessanywhere_second_factor_enabled`), the user is prompted to supply an authorization code (obtained from Helpdesk) or a Mobile ActiveCode (sent to a mobile phone).
- ❹ The user can now obtain the enterprise application passwords.

Recovery workflows for server issues

IMS Server is unavailable

Operational problem:

- The IMS Server is unavailable due to any of these problems: the IMS Server is down, the database server is down, or the data center is down.

Recovery workflow:

- ❶ The users can still log on to computers, provided that cached Wallets are available.
- ❷ Since the USB Key stores a cached Wallet, a user can log on with a USB Key, even if the IMS Server is unavailable.



If part of the Wallet is not stored on the USB Key (depending on `pid_usb_key_wallet_cache_option`), the user may not log on to the USB Key if the cached Wallet is not available on the computer.

- ❸ The Administrator should immediately recover the IMS Server, database server, or data center, so users without cached Wallets can log on to computers.
- ❹ The recovery procedures for a crashed IMS Server or database server are detailed in [The IMS Server has crashed](#) and [The database server has crashed](#).

The IMS Server has crashed

Prerequisites:

The IMS configuration files and keystores stored in these folders should be backed-up:

- IMS Installation Folder>\ims\certs\keystore
- IMS Installation Folder>\ims\config



The IMS keystores should be backed-up in a secure media. If the keystore is stolen and a hacker knows the passwords to those keystores, the hacker can set up a fake IMS Server, or may issue certificates using the certificate authority stored in those keystores, which are issued by Ecentuate Root CA.

Recovery workflow:

- ❶ If the IMS Server has stopped for some reason (e.g., a software bug) but there is no loss of files on the hard disk, the Administrator should restart the IMS Server.
- ❷ If the IMS Server executables, keystores, or configuration files are lost (e.g., due to a hard disk crash), the Administrator should restore from a backup (if available), or reinstall the IMS Server. Keystores and configuration files should be reinstated from the backup copies.
- ❸ Any changes to the configuration file between the crash and the last backup would be lost. As such, the Administrator must repeat these configurations.



If keystores cannot be restored (e.g., lost backup), they will need to be re-created. For more information, see [IMS keystore recovery](#).

The database server has crashed

Prerequisites:

- It is recommended to store IMS logs on a different database server from the IMS database. By using this setup, the transaction logs would still be intact if the IMS database (which contains the IMS system and user data) crashes.

Recovery workflow:

- ❶ If the database server has stopped for some reason (e.g., software bug), but there is no loss or corruption of data, the Administrator should restart the database server.
- ❷ In case of data loss or data corruption, the database should be restored from the latest backup.

- ③ The Administrator should then check the IMS logs to identify the transactions that have occurred between the crash and the last backup.
- ④ A recovery process can be defined for each transaction type. For example, if a user changes the Encentuate password after the last backup, the user would need to change the password again.

IMS keystore recovery

The IMS keystores stored in this folder (<**IMS Installation Folder**>\ims\certs\keystore) should be backed up in a secure media so that they can be restored in case the IMS Server's hard disk crashes.

If the keystores cannot be restored for some reason (e.g., lost backup), the recovery procedure described in this document must be invoked.

IMS has three (3) types of keystores that serve different purposes:

- CA keystore
- SSL keystore
- Log Signing keystore

There is also the **startup.file** file in the <**IMS Installation Folder**>\ims\certs\keystore folder that stores the password for encrypting all other passwords in the IMS configuration file. This startup password is used if the Administrator creates it during IMS installation.

Recovering the CA keystore

The IMS CA Keystore contains one entry for IMS Intermediate CA (a.k.a. IMS Soft CA), which is issued by IMS Root CA. Information of this intermediate CA is also stored in two database tables: **IMSCertServer** and **IMSTrustedCA**.

Below is a sample **IMSCertServer** table.

issuerDN	lastIssuedSerial Number	imsServer	Recovering the SSL keystore
CN=IMS Soft CA, O=ice-fall.corp.encentuate.com	133	icefall/10.1.16.6	100

In the **IMSCertServer** table, there is one row for each IMS Server. Typically, there is only one entry in the table, but in HA configuration, there might be more than one IMS Server, and each acts as one certificate authority server.

For each row, the **issuerDN** name should correspond to Distinguished Name (DN) of the intermediate CA. DN of the CA can be found in the subject field of the CA

certificate, which is usually **CN=IMS Soft CA, O=\${IMS_MACHINE_NAME}** and **\${IMS_MACHINE_NAME}** is usually IMS host name plus a windows domain name where IMS runs.

Below is a sample IMSTrustedCA table.

issuerDN	certificate_base64	type	expiration
CN=IMS Soft CA, O=ice- fall.corp.encyclopedia.com	-----BEGIN CERTIFICATE----- MIICGzCCAYSgAwIBAgICAcgwCwYJKo ZlhvCNAQEEMEoxEzARBgNVBAoTCmV uY2VudHVhdGUxHTAb BgNVBAsTFDAwMDAwMDAwMDAwMDAwMDAwMDAwMRQwEgYDVQQDEw tJTVMgUm9vdCBDQTAeFw0wNTA0 MTgxMTQ0MzBaFw0yMDA1MTgxMTQ 0MzBaMDwxJDAiBgNVBAoTG2ljZWZh bGwuY29ycC5lbmNlbnR1 YXRILmNvbTEUMBIGA1UEAxMLSU1TIF NvZnQgQ0EwgZ8wDQYJKoZIhvcNAQ EBBQADgY0AMIGJAoGB ALrnOWB7UIKik2L0kNr2v0xWUdyhVA 7KgcpcbpgHWqQKCEyH6Uv2Ez9Y01Cs 6He8jpOOieqVHNzEb 2LUWLJDKCnmQAtnmQTYGU4KWB2 4lakL+SYeH3O5GYcSMBCnj3rHHJv4U 2im05Mvm7/expOZOsv58 nSNAVLKZ1SFkY/eMvW/ pAgMBAAgjlDAeMA8GA1UdEwEB/ wQFMAMBAf8wCwYDVR0PBAQDAgE2 MA0G	IMSCA	5/18/2020 7:44:30 PM
CN=IMS Soft CA, O=ice- fall.corp.encyclopedia.com (continued)	CSqGSIlb3DQEBBAUAA4GBAB/ NZfsDa5xsqrnxA6FJztU2V0SVjxeqjNv7/ ehX4qjo/mCrAik76e2C qoLjDB6xCOgZBM+zvISnbxcOVJcMg6 JgFbjHRTJHt1Lx4y1kdZAYUtb1/nADT/ KWebyCb3fvTuOh GHTBnJlh2AKOdt8Nm4AiscDXZYb4LD 7ZD+PWd+6b -----END CERTIFICATE-----	IMSCA	5/18/2020 7:44:30 PM
.....

In the **IMSTrustedCA** table, there should be one entry for each intermediate CA. For each row, the **IssuerDN** name should correspond to Distinguished Name (DN) of the intermediate CA. The **certificate_base64** column should contain certificate of the CA, encoded in Base64 format. Type of each intermediate CA is **IMSCA**. The **expiration** column is the expiration time for the CA certificate.

To recover the CA keystore:

- ❶ If the original CA keystore is corrupted and a backup of the CA keystore is still available, the Administrator can overwrite the keystore with the backup copy. There is no need to change the IMS database.
- ❷ If the backup copy of the CA keystore is lost, the Administrator needs to re-generate a CA keystore (e.g., by reinstalling IMS and copying over the keystore). The **IssuerDN** column in the **IMSCertServer** table and **IssuerDN**, **certificate_base64** columns of **IMSTrustedCA** table must be updated.

Recovering the SSL keystore

The SSL keystore contains the SSL certificate of the IMS Server and its corresponding private key.

If the original SSL keystore is corrupted and a backup of the SSL keystore is still available, the Administrator can overwrite the keystore with the backup copy. There is no need to change the IMS database.

If the backup copy of the SSL keystore is lost, the Administrator must re-generate the SSL keystore (e.g., by reinstalling the IMS and copying over the keystore). Note that the **CN** field of the SSL certificate must match the **DNS name** of the IMS Server.

Recovering the log signing keystore

The Log Signing keystore contains secrets for hashing the IMS database logs and making them tamper-evident. The recovery process of this keystore is the same as that for SSL keystore. For more information, see [Recovering the SSL keystore](#).

Recovering the startup password

During IMS installation, the Administrator determines whether to set a password to protect the IMS Server. Once a password is set, the password will be required during IMS Server startup. The startup password is saved in the **startup.file** file, and encrypts all the passwords in the IMS configuration file.

In the IMS configuration file (**ims.xml**), if an entry in the **main** section is encrypted, it looks like:

```
<auth.otp.encryptKey>

<value xml:lang="en">#####encrypted####</value>
```

```
</auth.otp.encryptKey>
```

There is a corresponding entry in **< ciphertext>** section:

```
<auth.otp.encryptKey>
```

```
<value xml:lang="en">Ok/2+j8dWQN3pGp1y44tg+Fan86duOOw/  
wbmKcIrIdiQmweGpWWtLQ==</value>
```

```
</auth.otp.encryptKey>
```

If the **startup.file** file is corrupted or lost, the IMS Server cannot start since the encrypted passwords in the configuration file cannot be decrypted.

To recover the startup password:

- ❶ Manually reset all encrypted passwords in the IMS configuration file to plain text. The Administrator must know all these passwords.
- ❷ Create a new copy of the **startup.file** file and set the file with a new password.

PART V: ADVANCED CONFIGURATION

Part V: Advanced Configuration

Use this part of the guide to understand how to deploy Encentuate IAM Enterprise using other configurations. Refer to the following chapters:

- [AccessAgent for Citrix](#), which provides instructions on installing AccessAgent on a Citrix client and MetaFrame Server, logging in to MetaFrame, and policy settings for remote AccessAgent.
- [Roaming Sessions](#), which contains instructions on installing roaming sessions on Terminal Server or on Citrix.
- [Thin Client](#), which discusses how to set up the Thin Client of Encentuate IAM Enterprise, managing roaming sessions with RFIS, monitoring remote authentication devices and useful tips on managing the Thin Client system.

AccessAgent for Citrix

This chapter covers the following topics:

- [About Citrix MetaFrame](#)
- [Installing AccessAgent on a Citrix client](#)
- [Installing AccessAgent on a MetaFrame server](#)
- [Logging in to MetaFrame without local AccessAgent installed](#)
- [Logging in to MetaFrame without local AccessAgent installed](#)
- [Policy settings for remote AccessAgent](#)

About Citrix MetaFrame

Citrix MetaFrame provides a thin-client architecture to run and manage applications centrally on Windows 2000 or 2003 Server.

Encentuate integrates AccessAgent with the Citrix MetaFrame product suite to provide sign-on automation to applications running on Citrix servers.

In the integrated solution, AccessAgent runs within a Citrix MetaFrame session remotely on the Citrix MetaFrame server, and thus provides auto-capture and auto-fill of passwords.

The remote AccessAgent runs on the Citrix server, independent of whether there is a local AccessAgent running on the user's workstation. Both the local and remote AccessAgents synchronize credentials directly with the IMS Server.

For older installations of Citrix Server, be sure to turn on password encryption so that clear-text passwords will not be sent over the ICA channel. By default, newer installations of Citrix Server already have password encryption enabled.

This chapter provides an overview of various configurations and workflows involved in a Citrix deployment.

Installing AccessAgent on a Citrix client

Standard AccessAgent can be installed on the Citrix client.

Installing AccessAgent on a MetaFrame server

Standard AccessAgent can be installed on the Citrix server. The installer automatically installs the Citrix related components, if the computer has Citrix installed.

The following needs to be considered:

- **Do you want to replace Citrix server's GINA with Encentuate GINA?**

It is recommended not to replace GINA. The installer **SetupHlp.ini** file should be configured for this. That means when user directly connects to a Citrix Server without local AccessAgent, user will see Microsoft GINA's logon screen.



*For AccessAgent 3.3.0.0 and above, the behavior of the **EnginaEnabled** option in **SetupHlp.ini** is consistent for workstations, Terminal Servers, and Citrix servers. For Citrix servers, option **0** is recommended.*

- **How do you install Encentuate Network Provider DLL and enable it?**

An installer configuration is available in the file **SetupHlp.ini**. The default value of **1** should be used for the **EncentuateNetworkProviderEnabled** flag.

The machine policy **pid_en_network_provider_enabled** must be set to **1** as well. This can be set using AccessAdmin.

If the Encentuate Network Provider is not working as expected, follow these steps to see if it has been properly installed.

To check if the Encentuate Network Provider is properly installed:

- ❶ Check if the following registry key is present:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EnNetwork-Provider]

- ❷ Check the registry key:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order]"ProviderOrder"

Verify that **EnNetworkProvider** is listed. If not, add, **EnNetworkProvider** to the text. Do not include the comma if there are no preceding entries.

- ❸ Ensure that **EnNetworkProvider.dll** is in Encentuate installation directory (e.g., C:\Program Files\Encentuate).

A user can log on to the MetaFrame Presentation Server in two ways – through an ICA desktop client or via a web interface. The web interface uses a browser plug-in equivalent to the desktop ICA client.

The integrated workflow for the case when there is a local AccessAgent installed on the user's computer is very different from the case when there is no local AccessAgent. However, whether the user decides to log on through an ICA desktop client or through the web interface does not have an effect on the workflow.

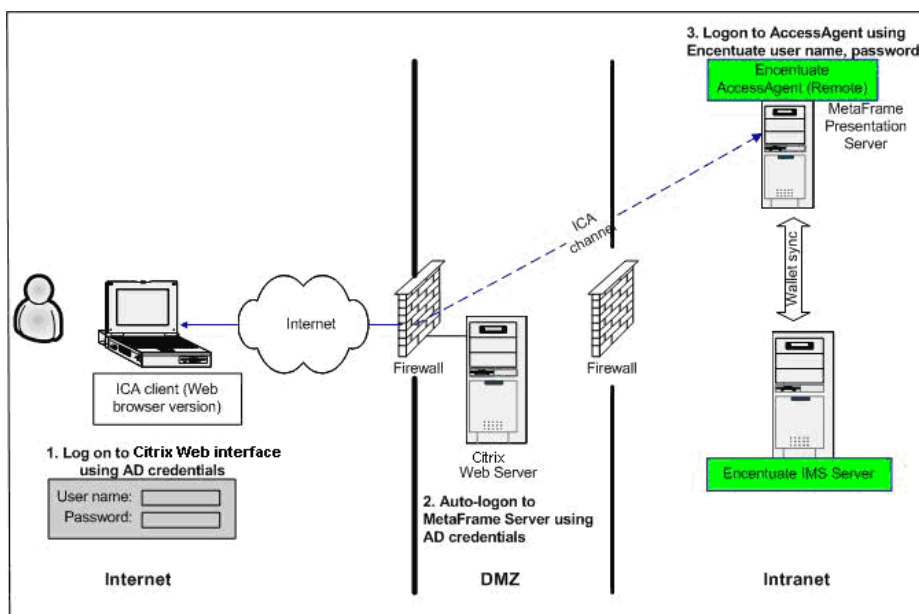
Logging in to MetaFrame without local AccessAgent installed

This workflow is primarily used from an extranet, usually for mobile users. For example, a doctor may log on to the Citrix Web interface from a computer in another hospital, where there is no AccessAgent deployed. Other examples include users logging on to a Citrix Web interface from home.

Based on the architecture diagram, there are three major steps involved:

- ❶ The user logs on to an Citrix Web interface using an Active Directory user name and password.
- ❷ After logging on, the user views a list of published applications. When launching an application, the Citrix Web Server automatically logs on to the MetaFrame Presentation server with the user's entered Active Directory credentials.
- ❸ After logging on to a MetaFrame server desktop, the user is automatically logged on to AccessAgent with the user's Encentuate user name and password, so remote AccessAgent can provide automatic application sign-on.

But the challenge is to capture the Encentuate user name and password for logging on to AccessAgent. Refer to the two possible solutions described in the next sections.



MetaFrame architecture diagram

Using the Active Directory password as the Encentuate password

In this solution, AccessAgent uses a **Network Provider** plug-in DLL called **EnNetworkProvider.dll**. This DLL captures the user's Active Directory user name and password when logging on to the MetaFrame server. The AccessAgent uses the Active Directory user name and password as the Encentuate user name and password for logging on to the user's Wallet. The entire logon process is seamless from the user's point of view.



For Citrix Web interface deployment, it is recommended to use this configuration, as this configuration offers the most seamless user experience.

Active Directory password synchronization should be enabled for this setup to function.

Do not use Active Directory password as Encentuate password

The user's Encentuate password and Active Directory password are not synchronized.

This option is considered inconvenient for the user, since the user must remember two sets of credentials, including the effort of logging on twice. This problem is also often referred as double-logon problem. There are two options provided to minimize the user inconvenience.

The logon process includes providing two (2) sets of credentials as follows:

- Active Directory user name and password for Citrix Web interface logon
- Encentuate user name and password for AccessAgent logon

Caching logon credentials on Citrix Server

In this option, the user must remember two (2) sets of credentials. However, the user enters only Active Directory credentials to log on, as the user's Encentuate logon credentials are retrieved automatically from the cached storage. Refer to the process outlined as follows:

- ① The user logs on to Citrix Web interface with Active Directory credentials.
- ② The user then clicks on a published application and the Citrix Web Server automatically logs on to the MetaFrame Presentation server with the user's Active Directory credentials (previously entered).
- ③ On the remote desktop, AccessAgent prompts the user for the Encentuate user name and password for the first time. AccessAgent caches the relevant logon credentials securely on the Citrix Metaframe presentation server so that AccessAgent can automatically log on to user's Wallet. The policies (**pid_ts_logon_prompt_enabled**, **pid_logon_user_name_prefill_option**, **pid_ts_logon_cache_enabled**) need to be configured for the logon prompt and caching options.

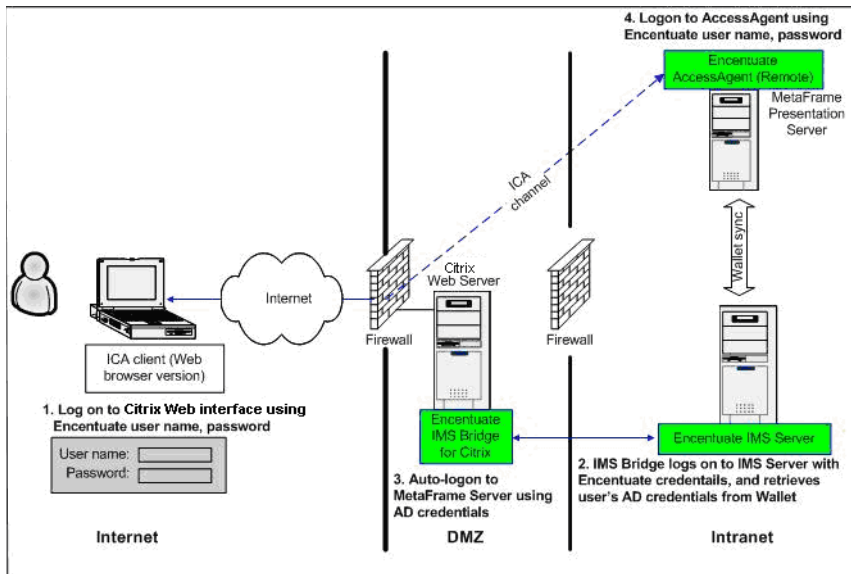
Tips:

- The user must remember two (2) sets of credentials, as both are needed for the very first logon.
- If the user changes the Encentuate password on another computer, the AccessAgent on Citrix server will not update changes in the cached storage. The user will be asked to enter the latest Encentuate password for the next Citrix logon.
- If there are multiple MetaFrame servers for a deployment, the user enter an Encentuate password for every new server, as the caching is done on the Citrix server locally.

Using a custom IMS Bridge (not recommended)

In this option, user does not need to remember two (2) sets of credentials. The user only needs the Encentuate user name and password.

Refer to the architecture diagram for this configuration. A custom IMS Bridge plugin is needed for the Citrix Web Server. However, the Encentuate IMS Bridge for Citrix is not a standard product component. The bridge needs to be customized by the Services team for each deployment.



Architecture diagram with IMS bridge

Based on the architecture diagram, there are four major steps involved:

- ❶ The user logs on to the Citrix Web Server using an Encentuate user name and password.
- ❷ The Encentuate IMS Bridge for Citrix intercepts the logon and logs on to the IMS Server using the Encentuate user name and password. The bridge retrieves the user's Active Directory credentials from the Wallet.
- ❸ After logging on to the Web interface, the user will see a list of published applications. When a particular application is launched, the Citrix Web Server automatically logs on to the MetaFrame Presentation server with the user's Active Directory credentials (as fetched by IMS Bridge).
- ❹ After logging on to the MetaFrame server desktop, AccessAgent prompts the user for the Encentuate user name and password for the very first time. AccessAgent caches the relevant logon credentials securely on the Citrix Metaframe Presentation Server so that AccessAgent can automatically log on to user's Wallet subsequently. The policies (`pid_ts_logon_prompt_enabled`, `pid_logon_user_name_prefill_option`, `pid_ts_logon_cache_enabled`) need to be configured for the logon prompt and caching options.

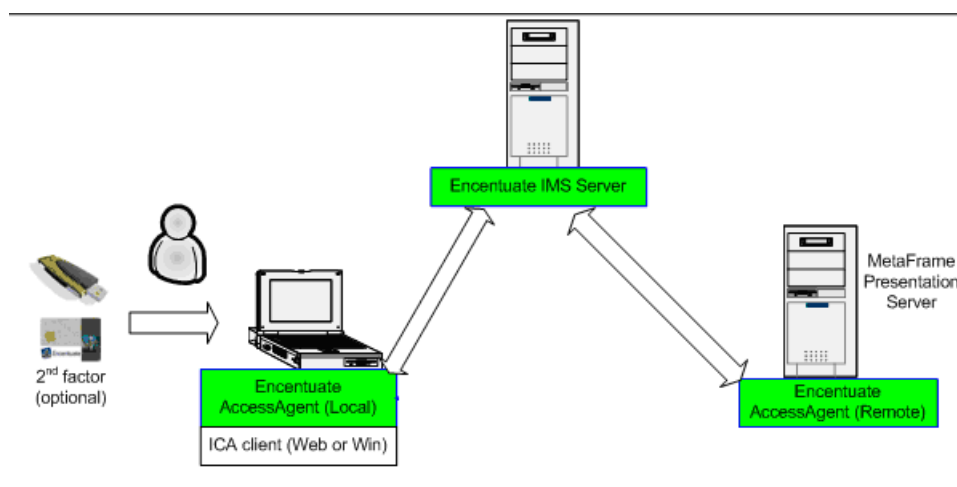
Tips:

- This setup needs a customized IMS Bridge.
- If the user changes the Encentuate password on another computer, the AccessAgent on Citrix server will not update the changes in the cached storage. The user must enter the latest Encentuate password for the next Citrix logon.

- If there are multiple MetaFrame servers for a deployment, the user must enter the Encentuate password for every new server, as caching is done on the Citrix server's local profile.

Logging in to MetaFrame with local AccessAgent installed

With AccessAgent installed and running on the user's local computer, the logon to the MetaFrame server will be seamless.



MetaFrame architecture diagram

Based on the architecture diagram above, the following steps are illustrated:

- 1 The user logs on to the local AccessAgent using an Encentuate user name and password. Based on the logon policy, the user may be required to present an authentication factor, such as an RFID card, USB Key, active proximity badge, or fingerprint.
- 2 The user launches the Citrix ICA client (Win or Web version) for the published application or for full desktop. The ICA logon screen is displayed.
- 3 The local AccessAgent then auto-fills with the Citrix logon credentials (usually the user's Active Directory account). The local AccessAgent will need an AccessProfile for the ICA client application.
- 4 The ICA client logs on to the Citrix server with auto-filled credentials.
- 5 If Active Directory password synchronization is enabled, the remote AccessAgent automatically logs on to user's Wallet using the ICA client's logon credentials, obtained from the Encentuate Network Provider.

However, if Active Directory password synchronization is disabled, the user needs to log on to remote AccessAgent manually using an Encentuate user name and password. Regardless of the user's Wallet authentication policy, the remote AccessAgent will always allow the user to log on with only the Encentuate user name and password.



If Active Directory password synchronization is not enabled, refer to [Caching logon credentials on Citrix Server](#) for an alternative option.

- ⑥ The remote AccessAgent attempts to retrieve the user's Wallet from the remote server's hard disk. If the user's Wallet is not cached, it tries to download from the IMS Server. The machine policy **pid_ts_wallet_caching_option** for the remote AccessAgent must be set to **2**, so remote AccessAgent can cache the user's Wallet on the hard disk. This is recommended to improve performance.
- ⑦ The remote AccessAgent provides automatic sign-on to applications running on the Citrix server.

The ICA desktop client for the published application must be configured so that when the user launches the client, the ICA client displays a local Windows GUI for the sign-on screen. Using AccessProfile, the local AccessAgent can auto-fill the right credentials.

If the ICA client does not display a local Windows GUI, it will directly connect to the Citrix Terminal Server and the Terminal Server's GINA logon screen will appear. The local AccessAgent cannot auto-fill with the logon credentials, as the remote screen appears as an image within the client.

Synchronizing Wallet contents

Depending on the usage, either the local or remote AccessAgent may capture new application accounts or modify certain credentials. The user must have a consistent view of the Wallet from any environment. Refer to these sections to know how the local and remote AccessAgents synchronize credentials through IMS Server.

Local AccessAgent and IMS Server synchronization

Upon logon, the local AccessAgent synchronizes the Wallet with the IMS Server. For any change during the AccessAgent session, the local AccessAgent updates the IMS Server on the change.

The local AccessAgent also does a complete re-synchronization of the Wallet with the IMS Server periodically, based on the policy **pid_wallet_sync_mins** (e.g., 30 minutes).

Remote AccessAgent and IMS Server synchronization

Upon logon, the remote AccessAgent synchronizes the Wallet with the IMS Server. For any change on the remote desktop, the remote AccessAgent updates IMS Server on the change. The remote AccessAgent also does a complete re-synchronization of the Wallet with IMS Server periodically, based on the policy `pid_wallet_sync_mins` (e.g., 30 minutes).



The synchronization of Wallet contents depends on both the local and remote AccessAgent’s ability to connect to the IMS Server. If one of the AccessAgents (e.g., local AccessAgent) cannot connect to the IMS Server, the local and remote AccessAgent will not have a consistent view of the Wallet if there are any changes.

Policy settings for remote AccessAgent

Policy ID	Machine policy of Citrix Server (configured through AccessAdmin)
<code>pid_logon_user_name_prefill_option</code>	2 (Prefill with currently logged on Windows user name)

Policy settings for remote AccessAgent, when Active Directory password is Encentuate password

Policy ID	Machine policy of Citrix Server (configured through AccessAdmin)
<code>pid_ts_logon_prompt_enabled</code>	1 (Yes)
<code>pid_ts_logon_cache_enabled</code>	1 (Yes)
<code>pid_ts_wallet_caching_option</code>	2 (Always cache)
<code>pid_logon_user_name_prefill_option</code>	2 (Prefill with currently logged on Windows user name)

Policy settings for remote AccessAgent, when Active Directory password is not Encentuate password; caching logon credentials enabled

Policy ID	Machine policy of Citrix Server (configured through AccessAdmin)
pid_ts_logon_prompt_enabled	1 (Yes)
pid_ts_logon_cache_enabled	0 (No)
pid_ts_wallet_caching_option	2 (Always cache)
pid_logon_user_name_prefill_option	2 (Prefill with currently logged on Windows user name)

Policy settings for remote AccessAgent, when Active Directory password is not Encrypted password; caching logon credentials disabled

Roaming Sessions

With roaming sessions, a user can disconnect from a desktop or application session from a client, log on to another client, and continue the desktop or application session in a new client. This setup is especially useful for a shared workstation environment, where users roam from one workstation to another, depending on the user's location at that point in time.

Encentuate AccessAgent is integrated with the RDP client, Terminal Server, ICA client, and Citrix server to provide sign-on automation to applications running on Terminal Servers or Citrix servers. In the integrated solution, the AccessAgent runs within a Windows session remotely on the Terminal Server or Citrix server, and auto-captures and auto-fills passwords. The remote AccessAgent communicates with the AccessAgent, if any, running on the user's local computer to synchronize credentials (only for Terminal Servers).

The chapter covers the following topics:

- [About roaming sessions](#)
- [System requirements](#)
- [Installing roaming sessions](#)

About roaming sessions

Terminal Server (TS) is Microsoft's thin-client architecture for running and managing applications centrally on the Windows Server (roaming session is only supported on Windows 2003 Server). While Citrix uses the Independent Computing Architecture (ICA) protocol for client-server communications, Terminal Server uses the Remote Desktop Protocol (RDP).

Citrix has the advantage of providing seamless access to published applications connecting to an entire remote desktop. Different applications can also be published on different Citrix servers, allowing the customer to decide which servers to allocate for each application. If the **seamless access to published applications** feature is not needed, Citrix can be configured to support roaming sessions, which is also supported by Terminal Server on Windows 2003 Server.

With thick clients (Windows 2000 or Windows XP), the local AccessAgent communicates with authentication hardware connected to a local (client) machine. For the user, second factor authentication is performed by the local AccessAgent. With Thin Clients (Windows CE or Windows XPe), there is no local AccessAgent. In this case, the remote AccessAgent directly communicates with the local authentication hardware to authenticate the user.

System requirements

The following table lists the roles supported combinations of clients, servers, and authentication factors:

Client Machine	Remote Server	Authentication Second Factors	Availability
Windows 2000 or Windows XP, with local AccessAgent	Terminal Server on Windows 2003	All second factors supported by AccessAgent	Available
Windows 2000 or Windows XP, with local AccessAgent	Citrix MetaFrame Presentation Server 3.0 on Windows 2003	All second factors supported by AccessAgent	Available
Windows 2000 or Windows XP, without local AccessAgent	Terminal Server on Windows 2003	Authorization code	Available
Windows 2000 or Windows XP, without local AccessAgent	Citrix MetaFrame Presentation Server 3.0 on Windows 2003	Authorization code	Available
Windows CE (Thin Client), without local AccessAgent	Terminal Server on Windows 2003	RF IDEas pcProx 232 reader (for 125 kHz cards)	Available
Windows CE (Thin Client), without local AccessAgent	Citrix MetaFrame Presentation Server 3.0 on Windows 2003	RF IDEas pcProx 232 reader (for 125 kHz cards)	Available

Installing roaming sessions

This section contains installation and configuration instructions for roaming sessions using Terminal Server or Citrix. It also contains some usage instructions for users, for the various alternative settings.

Installing roaming sessions on Terminal Server

Installing AccessAgent (Terminal Server)

- Install AccessAgent on the Terminal Server after Terminal Services has been enabled. The installer detects the Terminal Server and installs the required components accordingly. In particular, it automatically sets the **machine policy pid_machine_type_ts** to 1.
- Install AccessAgent on the client machines.
- Both local (on client) and remote (on server) AccessAgent must be configured to use the same IMS Server.



For older installations of Terminal Server, be sure to turn on password encryption so that clear-text passwords will not be sent over the RDP channel. By default, newer installations of Terminal Server already have password encryption enabled.

Terminal Services configuration

Enabling "Use client-provided logon info"

This setting ensures that credentials provided by the RDP client can be used to log on to TS. Some customers may have disabled this feature so as to prevent users from saving the credentials in the local workstation. There is a Microsoft hotfix that disables the saving of RDP credentials even if "Use client-provided logon info" is enabled. Refer to <http://support.microsoft.com/?kbid=839918> for details.

With this feature disabled, it is still possible to perform auto-logon for the RDP session by using the feature for Terminal Server auto-logon using EnGINA through collaboration between local and remote AccessAgent.

To enable "Use client-provided logon info":

- ① Launch **Terminal Services Configuration**.
- ② Right-click **RDP-Tcp** and select **Properties**.
- ③ Select the **Logon Settings** tab.
- ④ Mark the **Use client-provided logon info** checkbox.

How the RDP client performs auto-logon with "Use client-provided logon info" disabled:

- ① After launching RDP client, the remote Microsoft GINA is displayed within the RDP session.

- ❷ Local AccessAgent sends the user's Active Directory credentials over the RDP channel.
- ❸ The remote AccessAgent (EnGINA module) receives the user's Active Directory credentials from RDP channel and injects them into Microsoft GINA's logon prompt.

Disabling "Always prompt for password"

To disable "always prompt for password":

- ❶ Launch **Terminal Services Configuration**.
- ❷ Right-click **RDP-Tcp** and select **Properties**.
- ❸ Select the **Logon Settings** tab.
- ❹ Clear the **Always prompt for password** checkbox.

Enabling "Restrict each user to one session"

To enable "Restrict each user to one session":

- ❶ Launch **Terminal Services Configuration**.
- ❷ Click **Server Settings**.
- ❸ Mark the **Restrict each user to one session** checkbox.

Enabling auto-fill of Windows credentials in RDP Client

The user should auto-capture Windows credentials through Windows logon, RDP client, or any other application that require Windows credentials.

If Windows credentials are auto-captured through an RDP client, ensure that logon credentials are entered into the RDP client with **Options >>** clicked.

To auto-launch RDP client when local AccessAgent is logged on, create an AccessAgent logon script (**pid_script_logon_code**) that launches the RDP client (**mstsc.exe**) only if the session is a Console session (such as, local AccessAgent instead of remote AccessAgent). Below is an example logon batch script:

```
@echo off

if %SESSIONNAME%==Console start mstsc
```

AccessProfile for **RDP with Options** (`sso_site_wnd_rdp_with_options`) should be used, so that **Options >>** is always automatically clicked when the RDP client is launched. However, note that auto-logoff (such as, `pid_app_wallet_logoff_action`) should be disabled for this application. For more information, see [Application policy settings \(through AccessAdmin\)](#).

Terminal Server policy settings

Refer to these recommended policy settings. Some policies have a Notes section that indicate their dependencies and relationships with other policies.

Machine policy settings for remote AccessAgent (through AccessAdmin)

Policy ID	AccessAgent on server
<code>pid_machine_type_ts</code>	1 (Machine is Terminal Server)
<code>pid_ts_logon_prompt_enabled</code>	1 (Yes)
<code>pid_ts_logon_cache_enabled</code>	0 (No)
<code>pid_ts_wallet_caching_option</code>	2 (Always cache)
<code>pid_ts_engina_logon_no_local_session_enabled</code>	1 (Yes)
<code>pid_logon_user_name_prefill_option</code>	2 (Pre-fill with currently logged on Windows user name)

User policy settings (through AccessAdmin)

Policy ID	Shared workstations with all applications on server	Shared workstations with some applications on server	Personal workstations with some applications on server
<code>pid_ts_lock_local_computer_action</code>	No action	No action	No action
<code>pid_ts_logoff_local_session_action</code>	Log off remote AccessAgent and disconnect remote session	Log off remote AccessAgent and disconnect remote session	Log off remote AccessAgent and disconnect remote session
<code>pid_script_logon_enabled</code>	True	False	False
<code>pid_script_logon_type</code>	Batch	-	-
<code>pid_script_logon_code</code>	@echo off if %SESSION-NAME%==Con- sole start mstsc	-	-

Application policy settings (through AccessAdmin)

This setting is such so that the RDP client is controlled using the policy `pid_ts_logoff_local_session_action`.

Policy ID	Shared workstations with all applications on server	Shared workstations with some applications on server	Personal workstations with some applications on server
<code>pid_app_wallet_logoff_action</code> (for the RDP client)	Do nothing	Do nothing	Do nothing

To set the application policy through AccessAdmin:

- 1 Go to **AccessAdmin**.
- 2 Click **Application policies**.
- 3 Click on the application representing the RDP client. It may be called **Remote Desktop Connection** or a similar name.
- 4 Set **Action for the application, when user logs off AccessAgent** to **Do nothing**, and click **Update**.

Alternative policy settings (Terminal Server)

Instead of setting `pid_ts_lock_local_computer_action` to **Disconnect remote session**, `pid_ts_logoff_local_session_action` to **Log off remote AccessAgent and disconnect remote session**, and `pid_app_wallet_logoff_action` to **Do nothing**, you can also use the following alternative policy settings:

Policy ID	Shared workstations with all applications on server	Shared workstations with some applications on server	Personal workstations with some applications on server
<code>pid_ts_lock_local_computer_action</code>	No action	No action	No action
<code>pid_ts_logoff_local_session_action</code>	No action	No action	No action
<code>pid_app_wallet_logoff_action</code> (for the RDP client)	Close the application	Close the application	Close the application

To maintain roaming session capability, configure the Terminal Server session to disconnect when the connection is broken, which usually happens when the RDP client is closed.

To maintain roaming session capability (using Terminal Server Configuration user interface):

- ❶ Launch **Terminal Server Configuration**.
- ❷ Click **Connections**.
- ❸ Double-click **RDP-Tcp**.
- ❹ Click the **Sessions** tab.
- ❺ Under **When session limit is reached or connection is broken**, select **Disconnect from session**.

The same configuration can also be done using GPO settings, as detailed in this Microsoft knowledge base article:

<http://technet2.microsoft.com/WindowsServer/en/library/d74c8cc0-cd7c-484d-bc35-737d1bfd07a81033.mspx?mfr=true>



Only one (1) Terminal Server is currently supported.

Installing roaming sessions on Citrix

Installing AccessAgent (Citrix)

- Install AccessAgent on the Citrix server after the MetaFrame Presentation Server is installed. The installer detects the Citrix server and installs the required components accordingly. For example, it automatically sets the machine policy **pid_machine_type_ts** to 1.
- Install AccessAgent on the client machines.
- Both local (on client) and remote (on server) AccessAgent must be configured to use the same IMS Server.



For older installations of Citrix Server, be sure to turn on password encryption so that clear-text passwords will not be sent over the ICA channel. By default, newer installations of Citrix Server already have password encryption enabled.

MetaFrame Presentation Server settings

Disabling pass-through authentication

To disable pass-through authentication:

- ❶ Launch **MetaFrame Presentation Server Administration** (perform discovery if necessary).
- ❷ Expand *Suite Components >> Configuration Tools >> Web Interface*.
- ❸ Click the preferred Web Interface, then click **Configure authentication methods** and select **Explicit**.
- ❹ Click **config.xml** of desired Program Neighborhood Agent interface, then click **Configure authentication methods** and select **Prompt**.

Enabling Workspace Control

Use Workspace Control to activate disconnected applications.

To enable workspace control:

- ❶ Launch **MetaFrame Presentation Server Administration** (perform discovery if necessary).
- ❷ Expand *Suite Components >> Configuration Tools >> Web Interface*.
- ❸ Click the preferred interface, then click **Manage workspace control**.
- ❹ When using the **Program Neighborhood Agent**, right-click the **Program Neighborhood Agent** icon and select **Reconnect** to activate disconnected or active applications.
- ❺ When using the Web Interface, click **Advanced Options** on the logon page, and select **All applications** for the **Reconnects to:** option. Alternatively, click the **Reconnect** button after logging on to the Web Interface.

Published applications (Citrix)

- Use the ICA client or Web Interface (select the appropriate window display option) to configure for **seamless windows** or **non-seamless windows** mode for published applications.
- If possible, use the **non-seamless windows** mode so users can click the **Close** button of the **MetaFrame Presentation Server Client** window to disconnect.
- When using the Web Interface with **seamless windows** mode, applications can be disconnected by clicking the **Disconnect** button of the Web Interface page. Alternatively, right-click the **Web Client**, click **Open Connection Center**, select the appropriate Citrix server, and click **Disconnect**.

- When using the **Program Neighborhood Agent** with **seamless windows** mode, disconnect applications by right-clicking the **Program Neighborhood Agent**, and clicking **Disconnect**.

Terminal Services configuration

Enabling "Use client-provided logon info"

To enable "Use client-provided logon info":

- ① Launch **Terminal Services Configuration**.
- ② Right-click **ICA-Tcp** and select **Properties**.
- ③ Select the **Logon Settings** tab.
- ④ Mark the **Use client-provided logon info** checkbox.

Disabling "Always prompt for password"

To disable "always prompt for password":

- ① Launch **Terminal Services Configuration**.
- ② Right-click **ICA-Tcp** and select **Properties**.
- ③ Select the **Logon Settings** tab.
- ④ Clear the **Always prompt for password** checkbox.

Enabling "Restrict each user to one session"

To enable "Restrict each user to one session":

- ① Launch **Terminal Services Configuration**.
- ② Click **Server Settings**.
- ③ Mark the **Restrict each user to one session** checkbox.

Enabling auto-fill of logon credentials in ICA Client

The user should auto-capture logon credentials through ICA client, or any other application that requires ICA logon credentials (e.g., if ICA logon credentials are the same as Windows credentials, they can be auto-captured through Windows logon; AccessProfiles will need to be configured accordingly).

To auto-launch ICA client when logged on to local AccessAgent, create an AccessAgent logon script (**pid_script_logon_code**) that launches the ICA client (**pnagent.exe**) only if the session is a Console session (such as, local AccessAgent instead of remote AccessAgent).

Refer to the example logon batch script:

```
@echo off

if %SESSIONNAME%==Console start pnagent
```

Citrix policy settings

Refer to these recommended policy settings. Some policies have a Notes section that indicate their dependencies and relationships with other policies.

Machine policy settings for remote AccessAgent (through AccessAdmin)

Policy ID	AccessAgent on server
pid_machine_type_ts	1 (Machine is Terminal Server)
pid_ts_logon_prompt_enabled	1 (Yes)
pid_ts_logon_cache_enabled	0 (No)
pid_ts_wallet_caching_option	2 (Always cache)
pid_ts_engina_logon_no_local_session_enabled	0 (No)
pid_logon_user_name_prefill_option	2 (Pre-fill with currently logged on Windows user name)

User policy settings (through AccessAdmin)

Policy ID	Shared workstations with all applications on server	Shared workstations with some applications on server	Personal workstations with some applications on server
pid_script_logon_enabled	False	False	False
pid_script_logon_type	-	-	-
pid_script_logon_code	-	-	-

Application policy settings (through AccessAdmin)

This setting is such so that the Citrix ICA client is terminated by its AccessProfile (sso_site_wnd_citrix_ica_client) when user logs off AccessAgent.

Policy ID	Shared workstations with all applications on server	Shared workstations with some applications on server	Personal workstations with some applications on server
pid_app_wallet_logoff_action (for the Citrix ICA client)	Log off the application	Log off the application	Log off the application

Thin Client

This chapter covers the following topics:

- [About Thin Clients](#)
- [Enabling port redirection and mapping](#)
- [Setting the server's AccessAgent policies](#)
- [Starting up the Thin Client](#)
- [Managing roaming sessions with RFID](#)
- [Monitoring authentication devices on remote client machines](#)
- [Additional Thin Client tips](#)

About Thin Clients

Thin Clients are becoming more common in hospitals. Administrators usually run applications on Terminal Servers (TS) or Citrix Servers. Thin Clients are used as kiosk workstations. Users log on to TS or Citrix using Thin Clients.

However, Thin Clients do not have as much RAM or disk space like standard PCs and install software such as AccessAgent. It is also difficult to upgrade the software on a Thin Client.

In hospitals, Thin Clients (WinCE or WinXPe) from vendors like Neoware and Wyse are used as shared terminals. Since there is no local AccessAgent running on the Thin Clients, the server-side AccessAgent has to detect and verify authenticators, such as RFID cards, fingerprints, and smart cards.

This document presents the workflow, use cases, and related policy requirements for the development of Thin Client support for Encentuate AccessAgent.

Thin client PRD is related to roaming session (see [Roaming Sessions](#)).

Enabling port redirection and mapping

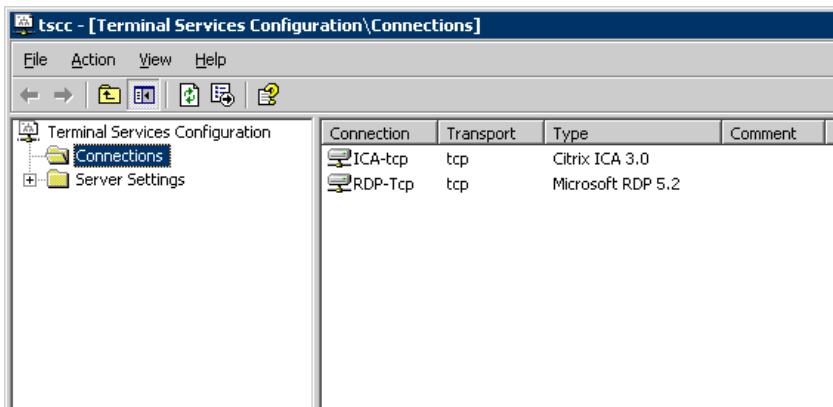
Configure the server based on your server connection. You can either use an ICA client or an RDP client for a Citrix server connection. If you are using an ICA client, follow the instructions in [ICA client connecting to a Citrix Server](#) section to configure your server. If you are using an RDP client, following [RDP client connecting to a TS/Citrix Server](#) section instead.

ICA client connecting to a Citrix Server

Follow the configurations below before installing AccessAgent on the Server:

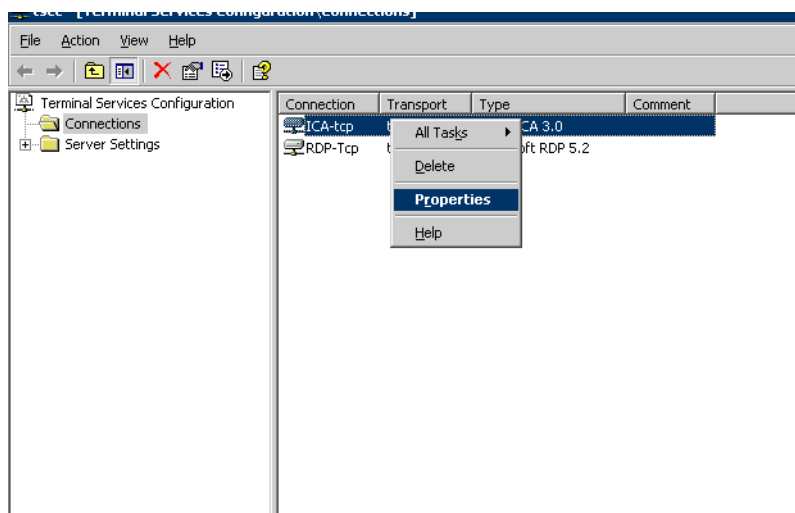
- ❶ On a Citrix Metaframe Server (Windows 2003 Server Operating System), login as the Administrator.

Click *Start >> All Programs >> Administrative Tools >> Terminal Services Configuration* to open the Terminal Service Configuration.



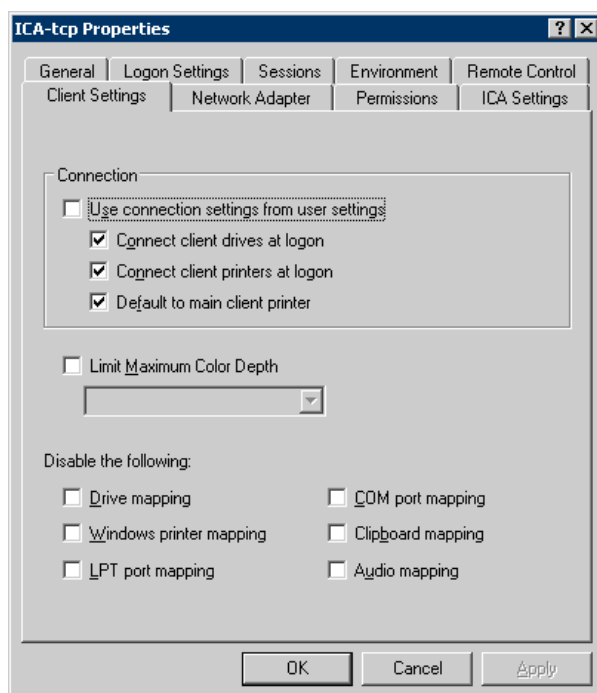
Selecting the Connections folder displays the ICA-tcp and RDP-tcp connection types

- ❷ For a Citrix server deployment, right-click on the **ICA-tcp** connection, and select **Properties**. The connection properties window should be displayed.



Right-click on the **ICA-tcp** connection, and select **Properties**

- 3 In the **ICA-tcp Properties** window, click the **Client Settings** tab and configure the settings under the tab as follows:



:Configure the settings in the Client Settings tab

- 4 Ensure that the **COM port mapping** is enabled (checkbox is cleared), since this is critical to the functioning of the AccessAgent. Click **Apply** to update the configuration. Logoff from the Windows session.
- 5 Verify the successful configuration. For more information, see [Testing Redirection of COM Port](#).

- 6 Add the following registry entries. These are explained in [Device Monitoring-Related Registry Entries](#) and are bundled into the `shared.reg` registry file that is mentioned in [Shared Workstation & Monitoring-Related Registry Entries](#).

[HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\SOCIMonitor]

"LocalVirtualComPort"=dword:00000001

"RemoteClientComPort"= the physical COM port number that the reader is connected to the Thin Client.

"MapRemoteClientComPortEnabled"=dword:00000001

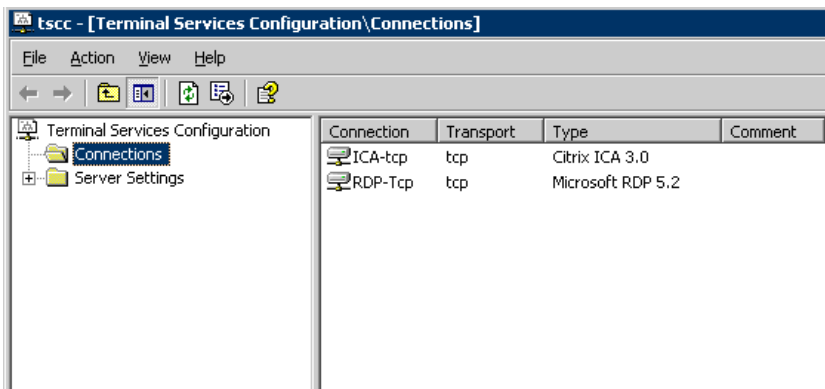
- 7 For the ICA client, you do not need to configure anything in order to achieve COM redirection (except for configuring it to auto-launch and auto-login to a pre-filled user account).

RDP client connecting to a TS/Citrix Server

Ensure that the following configurations are done before installing AccessAgent on the Server:

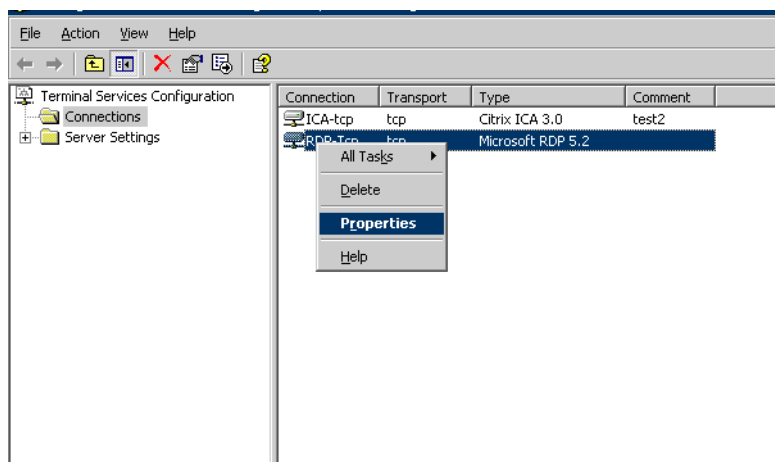
- 1 On a Terminal Server (Windows 2003 Server Operating System), log on as the Administrator and open the Terminal Service Configuration.

Click *Start >> All Programs >> Administrative Tools >> Terminal Services Configuration*.



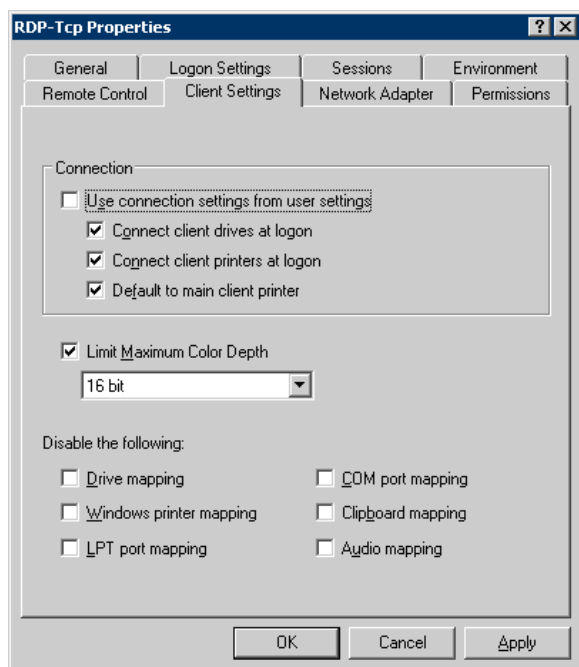
The connections tab should display at least the **RDP-Tcp** connection type

- 2 For a Terminal server deployment, right-click the **RDP-tcp** connection, and select **Properties**. The connection properties window should be displayed.



Right-click and select Properties

- 3 In the **RDP-Tcp Properties** window, click the **Client Settings** tab and configure the settings as follows:



Click the Client Settings tab and configure

Ensure that the COM port mapping is disabled (checkbox should be cleared), since this is critical to the AccessAgent function. Click **Apply** to update the configuration. Logoff from the windows session.

- 4 For an RDP Session, configure the client separately to redirect the communication port.

1. On the **Neoware Connection Manager** dialog box, click the **Configure** tab to configure an RDP connection if one does not already exist.
 2. Select the RDP connection and click **edit**.
 3. On the **local resources** tab, ensure that the **serial ports** checkbox is marked. The checkbox should read: **Connect automatically to these local devices when logged on to the remote computer**.
 4. Click **OK**.
- ❖ Verify the successful configuration. For more information, see [Testing Redirection of COM Port](#).

Setting the server's AccessAgent policies

To set the server's AccessAgent policies:

- ❶ After completing the previous procedures, install AccessAgent on the Server.
- ❷ Ensure that GINA has been replaced.
- ❸ Make sure the Winlogon registry key has a GinaDLL="engine.dll" value. Note for the Citrix Server, make sure that HKLM\software\Encentuate\PrevGINA = "ctxgina.dll". For more information, see [Configuring Auto-Logon to Servers](#) section.
- ❹ The Server must be configured as a shared workstation. The required registry configuration is provided in [Shared Workstation & Monitoring-Related Registry Entries](#). These settings must be made before starting the demo. Note that the appendix also contains registry entries pertaining to the card monitoring mechanism of AccessAgent.
- ❺ Restart the server machine.

Starting up the Thin Client

To start up the Thin Client:

- ❶ Set the connection to run automatically during startup on the client machine before starting up the Thin Client.
- ❷ Select the connection on the Neoware Connection Manager and click **Startup**.

- ③ Mark the **Automatically start the selected connection on startup** radio button from the popup menu.
- ④ In the **Configure** tab, edit the connection, mark **Automatic Logon** in the **General** tab, and fill out the corresponding credentials.

Use these credentials whenever this connection is used to connect to the server. Ensure that the server does not have any existing disconnected session for the same user. This will cause the client to reconnect to this existing session and port mapping will not work for ICA connections.

- ⑤ Run the Thin Client as described in the previous steps.

The Thin Client should automatically logon to the Server (ICA/RDP) and the Windows session should lock immediately.

Managing roaming sessions with RFID

AccessAgent supports roaming session from Thin Clients using RFID in the following manner:

- ① From a Thin Client, a Shared Desktop is automatically launched as an application through Citrix/Terminal Server.

This Shared Desktop serves as the default shared desktop for users on a Thin Client. Use the Thin Client's Windows credentials to create the Windows session on Citrix/Terminal Server that hosts this desktop. Assign a unique Windows user for each Thin Client.

- ② Configure the Shared Desktop (using Windows logon script defined through AD GPO) to lock the screen immediately after logon to display EnGINA. The user can then tap the RFID at the Thin Client and log on to AccessAgent in the Shared Desktop.
- ③ AccessAgent should automatically launch a Citrix/RDP session (User Desktop) from the Shared Desktop through an AccessAgent logon script. AccessAgent in the Shared Desktop injects the user's own Windows credentials in the Citrix/RDP client. This User Desktop can be hosted on the same or different Citrix/Terminal Server.
- ④ When the user finishes work on the User Desktop, the user can lock the screen or log off AccessAgent on the Shared Desktop. AccessAgent can be configured to close the User Desktop. The Citrix/RDP session hosting the User Desktop is now disconnected.
- ⑤ The user can log on to a Shared Desktop at another Thin Client and re-connect to the disconnected Citrix/RDP session.

To support the above workflow, `pid_ts_aa_menu_option` should be set to **2** (Always display all menu options).

Monitoring authentication devices on remote client machines

For AccessAgent on a Terminal Server or Citrix server, it may be required to monitor authentication devices on remote client machines (e.g., for Thin Clients where there is no local AccessAgent).

SOCIMonitor would map a virtual COM port on the Terminal Server (TS) or Citrix server to a physical COM port on the remote client. These settings are configured through registry values under the [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\SOCIMonitor] registry key.

Registry Value Name	Value Data (DWORD)	Description
MapRemoteClientComPortEnabled	1 0 (default: 1)	Whether the device monitoring mechanism should perform COM port redirection from the client machine (connecting to the TS) to the TS.
LocalVirtualComPort	Min 1 Max 8 (default: 1)	Virtual COM port on the TS to which data from the client COM port will get redirected to.
RemoteClientComPort	Min 1 Max unlimited (default: 1)	Physical COM port on the client to which the authentication device (e.g., RFID reader) is connected to. The redirection will take place from this port to the TS's virtual COM port.

Additional Thin Client tips

- ❶ Configure the server and client before the demo. When the demo is started, a startup of the client proceeds the locked GINA and the two factor Thin Client logon is best demonstrated.
- ❷ You must have two (2) registered users with badges. Log the badges on to the server at least once before the demo. This ensures that the Wallets are cached and there are no unnecessary delays during the demo.

- ③ Ensure that there are no existing sessions (for the credentials used to logon from the Thin Client) on the Citrix/TS Server when the client is first started up. For such cases, the client must reconnect to that session and locally tapped RFID badges will not work in that scenario.
 1. After auto-logging on to a Citrix/TS session using either ICA or RDP client, do NOT disconnect the session (do NOT click the **close** cross button of the ICA/RDP client). Once closed, the COM redirection will not be applied on the next session, and the RFID tap will not be redirected from the Thin Client to the remote server.
 2. If you accidentally disconnected the Citrix/TS session, reconnect to the previous session and then log off from that session (*Start >> Log Off*).
- ④ In some cases, the AccessAgent installer fails to register **ObsService.exe** as a service. This means that Web SSO will not work. The workaround is to register and start the service manually. The vb script `regObs.vbs` (in [VBScript for Registering and Starting ObsService](#) section) can be run on the machine to register, as well as start the service. After running the script, do a manual check to ensure that ObsService is registered and started.
- ⑤ For Web SSO to work, ensure that the **Enable Third Party Browser Extensions** option (under *InternetOptions >> Advanced*) is marked.
- ⑥ Be careful when you configure the RemoteClientComPort value as mentioned in [Device Monitoring-Related Registry Entries](#) and [Shared Workstation & Monitoring-Related Registry Entries](#) section. This value MUST be the physical port number that connects the reader to the Thin Client. In some cases, the value might work with the RDP client, but not the ICA client, or vice-versa. In this case, change the port number (typically 1 or 2 depending on how many ports there are on the Thin Clients) and see which one works.

APPENDICES

Appendices

Refer to the following appendices for more useful information on deploying Encentuate IAM Enterprise for your organization:

- [Appendix A: Deployment Tips](#)
- [Appendix B: Troubleshooting](#)
- [Appendix C: Definitions of policies](#)
- [Appendix D: Encentuate IMS Bridge for Citrix](#)
- [Appendix E: Creating a rule in MOM](#)
- [Appendix F: Mapping MOM Log Parameters to IMDS Server Log Attributes](#)
- [Appendix G: Testing Redirection of COM Port](#)
- [Appendix H: Device Monitoring-Related Registry Entries](#)
- [Appendix I: Shared Workstation & Monitoring-Related Registry Entries](#)
- [Appendix J: VBScript for Registering and Starting ObsService](#)
- [Appendix K: Configuring Auto-Logon to Servers](#)
- [Appendix L: Configuring MAC Settings at IMS Server](#)
- [Appendix M: Configuring a message connector](#)
- [Appendix N: Enabling MAC for Applications and Users](#)
- [Appendix O: Configuring the RADIUS Interface at IMS Server](#)
- [Appendix P: Integrating with Aventail SSL VPN](#)
- [Appendix Q: Integrating with Juniper SSL VPN](#)
- [Appendix R: Integrating with F5 SSL VPN](#)
- [Appendix S: Integrating an Application with MAC Using SOAP API](#)

Deployment Tips

The Administrator and Helpdesk Guides contain some useful configuration tips. This section lists additional tips that may be useful to professional services.

This appendix covers the following deployment tips:

- [Switching to another IMS Server](#)
- [Copying AccessProfiles between IMS Servers](#)
- [Deleting a user without revoking](#)
- [Promoting a user to Administrator](#)
- [Enabling/Disabling autoplay for removable drives](#)
- [Improving AccessAgent performance](#)
- [Specifying the IMS DB user account](#)
- [Configuring the ADAM Server](#)
- [Turning off authentication for AccessAdmin](#)
- [Configuring the IMS Server download port](#)
- [Enabling RFID readers for AccessAgent running in VMware](#)
- [Modifying AccessAdmin web pages](#)
- [Uninstalling AccessAgent in private desktops](#)
- [Private desktop with Websense internet content filtering services](#)

Switching to another IMS Server

To switch to a different IMS Server on the client machine:

- ❶ Set the machine policy `pid_ims_server_name` by editing the registry value [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\IMSService\DefaultIMSService]"ImsServerName".
- ❷ Download the IMS Server certificate by running: **C:\Program Files\Encentuate\SetupCertDlg.exe**.
- ❸ Log off AccessAgent (if logged on).
- ❹ Kill the AccessAgent processes: **AATray.exe**, **DataProvider.exe**, and **Sync.exe**.
- ❺ Stop the SOCIAccess service (**net stop sociaccess**).
- ❻ Delete the entire **C:\Program Files\Encentuate\Cryptoboxes** folder (backup the existing ones to another place if you intend to switch back to the original IMS Server).
- ❼ Restart the machine.

Restarting the machine with a missing machine Wallet will force AccessAgent to re-create the machine Wallet by downloading the latest policies and AccessProfiles from the current IMS Server.

To switch to a different IMS Server if you already have the Cryptoboxes for IMS Server backed-up:

- ❶ Log off AccessAgent (if logged on).
- ❷ Kill the AccessAgent processes: **AATray.exe**, **DataProvider.exe**, and **Sync.exe**.
- ❸ Stop the SOCIAccess service (**net stop sociaccess**).
- ❹ Restore the Cryptoboxes folder for the IMS Server (back up the existing ones to another location if you intend to switch back to the original IMS Server).
- ❺ Start the SOCIAccess service (**net start sociaccess**).
- ❻ Run **C:\Program Files\Encentuate\AATray.exe**.

Copying AccessProfiles between IMS Servers

To copy all AccessProfiles from one IMS Server to another:

- ❶ Set the machine policy `pid_ims_server_name` to the IMS Server which will contain the copied AccessProfiles.
- ❷ Run AccessStudio.

- ③ Perform a **Download from IMS Server**.
- ⑤ Save to a file (.eas extension) and exit AccessStudio.
- ⑥ Set the machine policy **pid_ims_server_name** to the target IMS Server.
- ⑦ Run AccessStudio.
- ⑧ Open the saved file.
- ⑨ Click **Upload All to IMS Server**.

Deleting a user without revoking

Once a user is revoked through AccessAdmin, the user name cannot no longer be used. To prevent a user name from being re-used, it is recommended to delete a user without revoking the user name.

To delete a user without revoking:

- ① Rename the user through AccessAdmin, by displaying the user's profile, modifying the user name (e.g., deleteduser94) and clicking **Update**.
- ② (Optional) Revoke the renamed user.
- ③ Remove any of the original user's cached Wallets that could be stored in the client PC's hard disks.

You can also enable the **Delete user** button in AccessAdmin using the IMS Configuration Utility (*Advanced Settings >> AccessAdmin >> User Interface >> Delete User Button*).

Promoting a user to Administrator

After signing up, a user is not assigned an Administrator or Helpdesk role unless previously configured as an Administrator during an IMS Server installation. A new Administrator is usually promoted to an Administrator role by existing Administrators through AccessAdmin.

If there are no more Administrators in the IMS database (e.g., the only Administrator has left the company and no one knows the password), existing users can be promoted to Administrator directly through the database.

To promote a user to Administrator directly through the database:

- ① Launch the database management user interface. The current user must have database Administrator rights.
- ② Open the **IMSIdentityUniqueAttribute** table to read off the **imsID** that refers to the target user.

- ③ Open the **IMSIdentityRole** table and set the **roleID** to **6** for the **imsID** identified earlier. The **roleID** of **6** is defined for **ImsAdmin** in the **IMSRole** table.

To promote a user to Administrator using the IMS CLTs:

- ① Launch command prompt and go to the **<IMS Installation Folder>\ims\bin** folder.
- ② Use **findAcct.bat <user name>** to obtain the **imsID**.
- ③ Use **addImsRole.bat <imsID> ImsAdmin** to promote user to Administrator.

Enabling/Disabling autoplay for removable drives

When an older version AccessAgent (before version 3.3.2.6) is installed, the installer sets a Windows registry entry called **NoDriveTypeAutoRun** to **4**, which disables autoplay when a removable drive is connected to the machine. If autoplay is enabled, Windows would activate autoplay every time a USB Key is inserted, which may not be necessary in some cases.

To disable Autoplay for removable drives:

- ① Remove the following registry entry or set it to 0:
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer]"NoDriveTypeAutoRun"
- ② Restart the machine.

For AccessAgent versions 3.3.2.6 and above, the installer no longer sets the **NoDriveTypeAutoRun** Windows registry entry. For USB Key deployments, set this policy using AccessAdmin.

Improving AccessAgent performance

The AccessProfiles can become very large data objects when they are parsed by the DataProvider process of AccessAgent. These data objects must be kept in memory. Removing unused AccessProfiles can speed up AccessAgent performance. To remove unused data objects, right-click on each unused AccessProfile and click **Delete**.

Specifying the IMS DB user account

Installation will fail if you specify the SA account as the IMS DB user account. The IMS DB user account should be different from the SA account.

Configuring the ADAM Server

It is recommended to read the ADAM Step-by-Step Guide from the Microsoft Download Center for detailed configuration instructions.

Refer to these topics for some quick tips on configuring ADAM so that the LDAP connector can connect to it using SSL.

Obtaining a certificate

To create a certificate, install IIS and Certificate Authority (*Control Panel >> Add/Remove programs >> Add/Remove Windows Components*).

For information on installing IIS, refer to Microsoft documentation or go to their website at <http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/iiiisin2.msp?mfr=true>.

To install a Certificate authority, mark the **Certificate services** checkbox.



IIS should be installed before or at the same time as you install the certificate services.

Once the installation is complete, request a certificate by browsing the following URL using Internet Explorer: <http://localhost/certsrv>.

To obtain a certificate:

- ❶ Click **Request a certificate**.
- ❷ Click **Advanced certificate request**.
- ❸ Click **Create and submit a request to this CA**.
- ❹ In the **Name** textbox, enter the full-qualified DNS name of the server.
- ❺ Make sure **Type of certificate** is **Server authentication certificate**.
- ❻ Select **PCKS10** as the format.
- ❼ Optionally fill in the other information.
- ❽ Click the **Submit** button.

To create a certificate:

- ❶ Open *Control Panel >> Administrative Tools >> Certification Authority*.
- ❷ Browse to the **Pending requests** folder.
- ❸ Locate the certificate request, right-click and select *All tasks >> issue*.

The certificate has now been created and it should reside in the **Issued certificates** folder.

To download and install the certificate:

- ❶ Go to <http://localhost/certsrv>.
- ❷ Click **View the status of a pending certificate request**.
- ❸ Click the certificate request.
- ❹ Click the certificate to install it.

Using the certificate with the ADAM service

To configure the ADAM service to use the certificate, place the certificate in the ADAM service's personal store.

To use the certificate with the ADAM service:

- ❶ Click *Start >> Run*, and enter **mmc** to launch the Microsoft Management Console.
- ❷ Click *File >> Add/Remove snap-in*.
- ❸ Click **Add...** and select **Certificates**.
- ❹ Select **Service account**.
- ❺ Select **Local computer**.
- ❻ Select your ADAM instance service.
- ❼ Add a new Certificate snap-in, but this time, select **My user account** instead of **Service account**.
- ❽ Click **Close** and **OK**.
- ❾ Open the **Personal** folder under the **Certificates - Current user** tree.
- ❿ Select the certificate and copy it into the same location under **Certificates - adam instance name**.
- ⓫ Give the ADAM service account read permissions to the key under **C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys**.



If these permissions are not set correctly, you will get an error in the event log: Schannel ID: 36870 - A fatal error occurred when attempting to access the SSL server credential private key. The error code returned from the cryptographic module is 0x6.

- ⓫ Restart your ADAM instance.

Verifying that SSL is working

To verify that SSL is working with ADAM:

- ❶ Run the **ADAM Tools Command Prompt** from your ADAM program group.
- ❷ Type **ldp** and press **Enter**.
- ❸ Click *Connection >> Connect...*
- ❹ Type the fully-qualified DNS name of your server in the server textbox (**local-host** will not work as the DNS name is checked against the certificate).
- ❺ Enter the SSL port of your ADAM installation (636 or 50001, or whatever you chose during the installation of ADAM).
- ❻ Mark the SSL checkbox and press **OK**.
- ❼ If the installation was successful, you should get a lot of text in the right window and can bind using the *Connection >> bind...* functionality.

Running ADAM service with a domain user account

To use a non-administrative domain user account (e.g., **domainUser1**) as the ADAM service account, make sure the following steps are performed.

To run ADAM service with a domain user account:

- ❶ Log on to Windows as **domainUser1** when requesting a server authentication certificate.
- ❷ In the certificate request page, mark the private key exportable.
- ❸ After installing the generated certificate into domainUser1's personal certificate store, open **Certificates** snap-in and export that certificate with private key.
- ❹ Log on to Windows as Administrator and use **Certificates** snap-in to import the certificate into ADAM service instance personal certificate store.
- ❺ When granting **domainUser1** read permission on private keys in **C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys**, set permission individually for each file as the permission on folder *MachineKeys* is not inherited.

Importing the root CA certificate into the IMS Server trust store

For the IMS Server to recognize the ADAM server when establishing an SSL connection, the root CA certificate for signing an ADAM server certificate must be imported into the IMS Server trust store. The import can be done by executing the following command:

```
keytool -import -file <path_to_exported_certificate> -keystore  
<path_to_ims_keystore> -alias <any_name> -storepass <password>
```

Restart the IMS Server after the certificate is imported.

Turning off authentication for AccessAdmin

By default, AccessAdmin is protected using SCR, which is a certificate-based authentication mechanism supported by AccessAgent. An Administrator must first log on to AccessAgent before accessing AccessAdmin.

For development or test IMS Servers, you can turn off authentication for AccessAdmin to simplify the configuration process.



You must never turn off authentication for production IMS Servers.

To turn off authentication for AccessAdmin:

- 1 Use the SQL Enterprise Manager (or equivalent tool) to insert the following data into the respective IMS database tables:

`imsID=IMSADMIN1` into the `IMSIdentity` table

`sociID=IMSADMINSID1` and `imsID=IMSADMIN1` into the `IMSSoci` table

`imsID=IMSADMIN1` and `roleID=6` into the `IMSIdentityRole` table
- 2 Modify the `web.xml` file in the `<IMS Installation Folder>\ims\WEB-INF` folder. Search for the following filter-mapping sections:

```
<filter-mapping>  
  
<filter-name>ScrFilter</filter-name>  
  
<url-pattern>/*</url-pattern>  
  
</filter-mapping>  
  
<!--  
  
<filter-mapping>  
  
<filter-name>NoAuthFilter</filter-name>
```

```

<url-pattern>/ui/admin/*</url-pattern>

</filter-mapping>

-->

```

- ❸ Comment out the "ScrFilter" and uncomment the "NoAuthFilter". The sections should look like this:

```

<!--

<filter-mapping>

<filter-name>ScrFilter</filter-name>

<url-pattern>/*</url-pattern>

</filter-mapping>

-->

<filter-mapping>

<filter-name>NoAuthFilter</filter-name>

<url-pattern>/ui/admin/*</url-pattern>

</filter-mapping>

```

- ❹ Save the modified **web.xml** file.
- ❺ Restart the IMS Server.

You should now access AccessAdmin without logging on to AccessAgent.

Configuring the IMS Server download port

If IIS or some other Web servers are installed on the same machine as the IMS Server, it may be necessary to use a download port other than the default port 80. Configuration changes must be done on both the IMS Server and AccessAgent.

The IMS Server HTTP port must be changed from 80 to another port (e.g., 88) in the **server.xml** file located at **<IMS Installation Folder>\conf\server.xml**. In the section regarding the service **tomcat-standalone**, make the following changes. Restart the IMS Server after the change is done.

```

<Connector
className="org.apache.coyote.tomcat4.CoyoteConnector"

    port="88" minProcessors="5" maxProcessors="75"

    enableLookups="false" redirectPort="443"

    acceptCount="100" debug="0" connectionTimeout="20000"

```

```
useURIVValidationHack="false" disableUploadTimeout="true" />
```

Modify the **ImsDownloadPortDefault** entry in the **SetupHlp.ini** file of the AccessAgent installer, then install AccessAgent. Alternatively, if AccessAgent has already been installed, you can modify the registry key [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\IMSService\DefaultIMSSettings] ImsDownloadServicePort.

To delete any existing cached Wallets:

- ❶ Log off AccessAgent (if logged on).
- ❷ Kill the AccessAgent processes: **AATray.exe**, **DataProvider.exe**, and **Sync.exe**.
- ❸ Stop the SOCIAccess service (**net stop sociaccess**).
- ❹ Delete the entire **C:\Program Files\Encentuate\Cryptoboxes** folder.
- ❺ Restart the machine.

Enabling RFID readers for AccessAgent running in VMware

Since the RFID reader is actually a Human Interface Device (HID), the following line should be added to the VMware image's VMX file: **usb.generic.allowHID = "TRUE"**.

Modifying AccessAdmin web pages

Starting from IMS Server 3.5.0, JSPs are pre-compiled when an IMS Server is installed or upgraded. This is to improve the loading speed of IMS Server pages (AccessAdmin and IMS Configuration Utility) on first access.

Since the JSPs are pre-compiled, they cannot be edited or replaced without re-starting IMS Server. Furthermore, the compiled JSP class also needs to be replaced and IMS Server needs to be re-started for the change to take effect.

Alternatively, you can exclude any of the JSPs from the pre-compilation requirement by modifying the **<IMS Installation Folder>\ims\WEB-INF\web.xml**.

To modify AccessAdmin web pages:

- ❶ Search for the JSP file that you want to modify in **web.xml** (e.g., **indexAlt.jsp**).
- ❷ Comment out the entire servlet-mapping section for the JSP file by adding "**<!--**" at the beginning and "**-->**" at the end. For example:

```
<!--<servlet-mapping>

<servlet-name>ui.indexAlt_jsp</servlet-name>

<url-pattern>/ui/indexAlt.jsp</url-pattern>
```

```
</servlet-mapping>-->
```

- 3 Save the modified **web.xml** file and restart the IMS Server.

Uninstalling AccessAgent in private desktops

To perform certain administrative actions, such as installing and uninstalling applications, usually the local Administrator account must be running in the Default desktop, which is the desktop assigned to the first logged-on user.

However, for private desktops, the auto-admin logon account may not have Administrator rights.

To uninstall AccessAgent in a private desktop, do either of the following:

- Restart the machine, press and hold the **Shift** key until Microsoft GINA appears, then log on manually as Administrator.
- Connect to the machine through remote desktop (RDP) and log on as Administrator.



The second method is only applicable to AccessAgent 3.6 and higher versions.

Private desktop with Websense internet content filtering services

For deployments using Internet content filtering services (e.g., Websense), a handful of commands in an Internet router prompts to check with the filtering service and database before permitting any web traffic to pass. Filtering is almost purely based on Active Directory groups; there are a few physician office VLANs filtered based on IP range.

The Encentuate machines are passing the credentials of the generic login account to Websense for filtering purposes, rather than the account of the end user that is using IE on the machine.

Users who cannot be identified through transparent authentication (or users sharing a computer such as in a Windows Terminal Services) are filtered by workstation or network policies, or by the Global policy. Users on shared machines cannot be filtered by policies assigned to directory objects. Websense is only identifying the first user to logon to the workstation and not recognizing any subsequent logons.

To resolve the issues, use one of the supported proxy servers that authenticate users (e.g., Microsoft ISA Server, Microsoft Proxy Server).

For more information, go to the following site: <http://www.websense.com/SupportPortal/SupportKBs/1223.aspx>.

Troubleshooting

Refer to the following topics to find a solution to specific issues:

- [AccessAgent logs](#)
- [AccessAgent log level](#)
- [IMS Server console](#)
- [Downloading the IMS Server certificate](#)
- [Unable to connect to the IMS Server](#)
- [AccessAgent cryptoboxes](#)
- [Machine Wallet download problem](#)
- [Unable to log on to AccessAdmin](#)
- [Synchronization with IMS Server](#)
- [Logon user interface failed to load](#)
- [AccessAgent does not display the correct domain](#)
- [Cannot return to EnGINA from Windows GINA](#)
- [Web automatic sign-on fails on Internet Explorer settings](#)
- [Automatic sign-on does not work properly for Windows applications](#)
- [Modification to Winlogon AccessProfile does not take effect](#)
- [Back button does not work for AccessAdmin, AccessAssistant, and Web Workplace](#)
- [IMS Configuration Utility cannot be accessed after the IP address has changed](#)
- [IMS Server cannot issue certificate for an application](#)
- [IMS Server diagnostic information](#)

- [IMS Server database housekeeping problems](#)
- [Anti-virus software may interfere with AccessAgent or IMS Server](#)
- [MSDE installation problem](#)
- [IMS Server installation problem due to database configuration](#)
- [Failure to connect to named instance of SQL Server 2000 database](#)
- [Cannot log on to Wallet after AccessAgent is installed](#)
- [Application is slower when automatic sign-on is enabled](#)
- [Missing labels in state engine view of AccessStudio](#)
- [Spontaneous termination of sync.exe](#)
- [GINA conflict with ThinkPad fingerprint software](#)
- [AccessAgent fails to install](#)
- [Cannot log on to cached Wallets](#)
- [A message, "Microsoft SQL Server 2000 SP3a or above required" displayed when installing MOM 2005](#)
- [A message, "Failed to create data source for data warehouse" displayed when installing MOM Reporting](#)
- [Performance data is not available in MOM reports](#)

AccessAgent logs

To troubleshoot AccessAgent problems, it is useful to view the log files in **C:\Program Files\Encentuate\logs** folder. XML files indicate communications with the IMS Server and are useful for troubleshooting failure due to AccessAgent-IMS Server interaction. **AccessAgent.log** logs internal AccessAgent processes and are useful for troubleshooting internal failure in AccessAgent. **aa_observer.log** logs the observation of applications for automatic sign-on.

For installation problems, the AccessAgent installer logs can be found in **C:\AAInstaller.log**.

When reporting a bug, it is useful to include a zip file that contains the entire **C:\Program Files\Encentuate\logs** folder. Provide the approximate local times when the events occurred.

AccessAgent log level

To troubleshoot AccessAgent problems, it is useful to increase the log level so that more debugging information can be produced.

The log level is specified by the machine **policy pid_log_level**, which can be set through the registry entry
[HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\DeploymentOptions]"LogLevel"
.

Log level 3 is usually enough for most debugging purposes. If more detailed logs are required, the log level can be set to 4.

IMS Server console

By default, the IMS Server runs automatically as a service **IMSService** when the server starts up. When in this mode, it may be difficult to troubleshoot any problems with the IMS Server. Alternatively, the IMS Server can be run in console mode so that any error messages are displayed in real-time.

To run the IMS Server in console mode:

- ❶ Stop the IMSService (**net stop IMSService**).
- ❷ Run the batch file: **<IMS Installation Folder>\ims\bin\runserver.bat**.

Downloading the IMS Server certificate

If configured properly, the AccessAgent installer should download the IMS Server certificate to the client PC. However, this download may fail if the client PC is offline or the IMS Server is not available at that time. The server certificate can be downloaded after installation through any of the following methods:

- *Start >> All Programs >> Encentuate AccessAgent >> Set IMS Server Location*
- Running **C:\Program Files\Encentuate\SetupCertDlg.exe**

Unable to connect to the IMS Server

If AccessAgent cannot connect to the IMS Server, it cannot perform certain operations, such as:

- Logging on to AccessAgent when there is no existing cached Wallet for the user
- Changing an Encentuate or USB Key password
- Registering a second factor
- Signing up users

The following situations could prevent AccessAgent from connecting to IMS Server:

- The client machine is not on the network.
- The client machine has no network connectivity (or lost connectivity) to the IMS Server. This could be due to an intervening firewall between the client machine and the IMS Server, or due to some network configuration issues, such as DNS problems.
- The client machine has a personal firewall or anti-spyware that is blocking traffic from AccessAgent. To allow AccessAgent to contact the IMS Server while computer is locked, the personal firewall or anti-spyware must also not be blocking traffic from **winlogon.exe**.
- The client machine does not have the IMS Server certificates installed, possibly because the client machine was offline during AccessAgent installation (see [Downloading the IMS Server certificate](#)).
- AccessAgent registry settings are corrupted or misconfigured (e.g., AccessAgent is pointing to the wrong IMS Server).

AccessAgent cryptoboxes

AccessAgent stores user and machine Wallets as hidden files in the **C:\Program Files\Encentuate\Cryptoboxes** folder. The machine Wallet (**C:\Program Files\Cryptoboxes\Wallets\machine.wlt**) contains system policies and AccessProfiles downloaded from the current IMS Server. To view the Wallet files, make sure that Windows explorer has been configured to **Show hidden files and folders**.

To refresh the user Wallets during testing or troubleshooting, delete the corresponding Wallet files in the **C:\Program Files\Encentuate\Cryptoboxes\Wallets** folder.

To refresh the machine Wallet, refer to the next procedure. The SOCIAccess service automatically replaces any deleted machine Wallet file, so deleting a folder (as with user Wallets) will not achieve the same result.

To refresh the machine Wallet:

- ❶ Log off AccessAgent (if logged on).
- ❷ Kill the AccessAgent processes: **AATray.exe**, **DataProvider.exe**, and **Sync.exe**.
- ❸ Stop the SOCIAccess service (**net stop sociaccess**).
- ❹
- ❺ Delete machine Wallet.
- ❻ Restart the machine.

Restarting the machine with a missing machine Wallet will prompt AccessAgent to re-create the machine Wallet by downloading the latest policies and AccessProfiles from the current IMS Server.

Machine Wallet download problem

When a machine starts up with a missing machine Wallet, AccessAgent attempts to create the machine Wallet by downloading the latest policies and AccessProfiles from the current IMS Server.

However, if the IMS Server is inaccessible, AccessAgent uses the policies and AccessProfiles specified in the following file: **C:\Program Files\Encentuate\all_sync_data.xml**.

To confirm whether the machine Wallet has been downloaded properly, run AccessStudio, load AccessProfiles from AccessAgent, and then click on **sso_site_web_ims_admin** under AccessProfiles. The machine Wallet is correct if the **@domain** field on the right panel is set to the IMS Server name. If the **@domain** field is **\$hostname**, the machine Wallet has not been downloaded properly.

If AccessAgent cannot successfully download the policies and AccessProfiles from the IMS Server despite several manual synchronization attempts, you can edit the policies and AccessProfiles directly in the **all_sync_data.xml** file.

To refresh the machine Wallet:

- ❶ Log off AccessAgent (if logged on).
- ❷ Kill the AccessAgent processes: **AATray.exe**, **DataProvider.exe**, and **Sync.exe**.
- ❸ Stop the SOCIAccess service (**net stop sociaccess**).
- ❹ Delete machine Wallet.
- ❺ Restart the machine.

For some deployments, workstations can only connect to the network after a user logs on to Windows. Since AccessAgent needs to download system data from the IMS Server during first startup after installation, other workstations will be unsuccessful in connecting at that time. For this reason, AccessAgent is inaccessible on first startup.

A workaround is for the first user to bypass EnGINA and log on to Windows directly. After that, subsequent users can log on normally through EnGINA. Another alternative is to include the IMS Server's latest **all_sync_data.xml** file in the installation package.

To include the all_sync_data.xml file in the installation package:

- ❶ Launch AccessStudio.
- ❷ Click **Tools >> Backup System Data from IMS to File**.
- ❸ Click **Backup**, and save it as **all_sync_data.xml**.

- ④ Place **all_sync_data.xml** in the **Config** folder of the AccessAgent installer package.

Unable to log on to AccessAdmin

If a user cannot log on to AccessAdmin, check the following:

- Make sure that the user has an Administrator or Helpdesk role.
- If the user is not using a USB Key, ensure that user's Wallet has been cached.



AccessAdmin logon requires certificate authentication, which is only available for a cached Wallet or USB Key.

- Make sure that the machine wallet has been downloaded properly (see [Machine Wallet download problem](#)).
- Make sure that the DNS name of the IMS Server does not contain the "_" character (see [Machine Wallet download problem](#)).
- Make sure that the URL of AccessAdmin is the same URL specified during IMS installation. To check the setting, go to the IMS Server page and double-click on the little lock icon to view the SSL certificate. The SSL certificate should list the exact hostname that you have to use.
- If you are using Windows 2003 and the homepage of Internet Explorer starts up with the page **res://../hardAdmin.htm**, the **Advanced Security Option** may be enabled.

To set the homepage to **res://../softAdmin.htm**, go to the **Add/Remove programs** menu from the **Control Panel** and choose to **Add/remove Windows components**. Remove the **Internet Explorer Enhanced Security Configuration**.

Synchronization with IMS Server

AccessAgent performs synchronization with the IMS Server periodically according to the frequency specified by **pid_wallet_sync_mins**. It is sometimes useful to invoke synchronization manually so the latest policies or AccessProfiles can be downloaded. This is especially useful during troubleshooting or demos.

To enable the AccessAgent right-click option for **Synchronize with IMS**, set the machine policy **pid_wallet_manual_sync_enabled** to 1, which can be set through the registry entry
[HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\Temp] "WalletManualSyncEnabled".

Logon user interface failed to load

Upon startup, instead of EnGINA, the following error message appears:

Caption: User Interface Failure

Message: The Logon User Interface DLL xxx.dll failed to load...

Either EnGINA has not been properly installed or the Winlogon GINA registry entry was not set correctly after AccessAgent was uninstalled.

To resolve the problem:

- ❶ Restart the computer.
- ❷ Go to **Safe Mode** by pressing **F8** before Windows starts up.
- ❸ Log on as an Administrator.
- ❹ Modify the following Windows registry value:
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]"GinaDLL".
- ❺ If the value was **engina.dll**, EnGINA was probably not installed properly and could not load. Change the value to **msgina.dll**. The default Windows Logon prompt will be displayed on startup.
- ❻ To use EnGINA again after fixing the problem, change the value to **engina.dll**.

AccessAgent does not display the correct domain

■ For IMS Server version 2.x

When a user logs on, AccessAgent shows the display name of the authentication service specified by **pid_bind_auth_list** in the **Domain** field. To modify the displayed domain, use AccessStudio or the IMS Configuration Utility to modify the display name of the appropriate authentication service.

■ For IMS Server version 3.x and above

The policy **pid_bind_edir_list** replaces **pid_bind_auth_list**. AccessAgent shows the domains specified in the enterprise directory listed in **pid_bind_edir_list**.

Cannot return to EnGINA from Windows GINA

Users cannot return to EnGINA from Windows GINA by clicking the **Cancel** button if the following domain group policy is set to "Enabled":

[Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options]

"Disable CTRL+ALT+DEL requirement for logon".

To fix this problem, set the value to **Disabled** or **Not Defined**.

Web automatic sign-on fails on Internet Explorer settings

Due to a Microsoft bug (<http://support.microsoft.com/?kbid=316593>), Internet Explorer 5.5 with Service Pack 2 and Internet Explorer 6.0 without Service Pack cannot be used with AccessAgent. Users need to upgrade their Internet Explorer to at least 6.0 with Service Pack 1.

Web automatic sign-on will also fail if Internet Explorer has been configured to disable third-party browser extensions.

To enable third party browser extensions in Internet Explorer:

- ❶ In Internet Explorer, go to *Tools >> Internet Options >> Advanced*.
- ❷ Under the **Browsing** category, look for **Enable third-party browser extensions (requires restart)**. Mark the option and click **OK**.
- ❸ Exit Internet Explorer and try Web automatic sign-on again.

It is also possible for some spyware to automatically remove the Encentuate Browser Helper Object. For such cases, Web automatic sign-on may initially work, and not work subsequently. Install and run an anti-spyware software to clear all spyware in your machine before re-installing AccessAgent.

Automatic sign-on does not work properly for Windows applications

The required services may not have been registered properly during AccessAgent installation.

To register the required services:

- ❶ Launch the command prompt (*Start >> Run >> cmd*).
- ❷ Go to the Encentuate program directory (*cd C:\Program Files\Encentuate*).

```
obsservice -service  
  
regsvr32 -i winsssoagent.dll  
  
net start obsservice
```

Automatic sign-on does not work properly for Microsoft GINA

For IMS Server versions between 3.1.1.6 and 3.1.7.1, the domain name must be regenerated for the authentication service representing the Windows credentials.

When you configure an enterprise directory for an Active Directory server, IMS Server automatically generates authentication services, one for each Active Directory domain.

To view the auto-generated authentication services in the IMS Configuration Utility, click **Authentication Services** in the left panel and select the authentication service from the drop down list.

For an authentication service representing an Active Directory domain, two domain names are included in the **Server locators to be used during injection**: one is the DNS domain name (e.g., test.encentuate.com), while the other is the NETBIOS domain name (e.g., encentuate_test).

To perform automatic sign-on at Microsoft GINA, ensure that the NETBIOS domain is the first item in the list.

Modification to Winlogon AccessProfile does not take effect

The latest AccessProfile of an application is loaded when the application process starts. Since the Winlogon process is only started on machine startup, restart the machine for the new Winlogon AccessProfile to take effect.

Back button does not work for AccessAdmin, AccessAssistant, and Web Workplace

The browser's **Back** button cannot be used when accessing AccessAdmin, AccessAssistant, and Web Workplace. AccessAssistant and Web Workplace are designed this way for security reasons, whereas AccessAdmin is designed this way due to certain implementation constraints.

IMS Configuration Utility cannot be accessed after the IP address has changed

If the IP address of the IMS Server has changed, the IMS Configuration Utility is inaccessible from http://imsservername:8080/, unless the new IP address is included in the **RemoteAddrValve** configuration key of the **<IMS Installation Folder>\conf\server.xml** file. Restart the IMS Server after the configuration key is modified.

Alternatively, to retain the original configuration key, you can still access the IMS Configuration Utility from http://localhost:8080/.

IMS Server cannot issue certificate for an application

It is a known bug that subject fields of IMS certificates can not contain the "_" character. This may cause problems at deployments that use certificate authentication for applications.

The result is that IMS Server cannot issue SCR or CAPI certificates for an authentication service with ID that contains the "_" character. The workaround is to remove all "_" characters from the IDs of authentication services that use certificate authentication.

IMS Server diagnostic information

The IMS Server diagnostic information can be obtained at the URL: <https://imsserver/ims/ui/diagnostics>. Note that you should first log on to AccessAdmin before navigating to this page.

The site contains the list of SOAP services, IMS configuration information, test facilities for IMS Connectors, and descriptions of event and result codes.

IMS Server database housekeeping problems

For normal database backup operations, the IMS database user must have backup permissions on the IMS database. However, if the Housekeeping RDB System Backup Flag is set to true, the IMS database user also need administrative privileges, otherwise the following exception appears in the IMS Server standard error logs:

```
java.sql.SQLException: [Microsoft][SQLServer 2000 Driver for
JDBC][SQLServer]BACKUP DATABASE permission denied in database
'master'.
```

If **cleanupRdbLogs** is enabled (i.e., log table pruning), a **logs** directory should exist in the <IMS Installation Folder>\bin directory, otherwise the following exception appears in the IMS Server standard error logs:

```
java.io.FileNotFoundException: logs\rdbLogCleanup.log (The
system cannot find the path specified)
```

Anti-virus software may interfere with AccessAgent or IMS Server

Some anti-virus software have been observed to interfere with AccessAgent or IMS Server, causing the following symptoms:

- AccessAgent (on user's PC, terminal server, or Citrix server) may become very slow.
- AccessAgent (on user's PC, terminal server, or Citrix server) may fail to start.
- Logging on to AccessAgent (on terminal server or Citrix server) may fail intermittently.
- The IMS Server may become very slow.

At present, the above problems have been observed at deployments that use McAfee anti-virus. To resolve the problem, store the frequently changing Encentuate folders (C:\Program Files\Encentuate\logs for AccessAgent, and C:\Encentuate for IMS Server) in the anti-virus software's exclusion list. For McAfee, refer to the next procedure.

To include Encentuate folders in an antivirus software's exclusion list (McAfee):

- ❶ Open the scanner's property pages.
- ❷ On the **Detection** tab, under **What not to scan**, use the exclusions feature.
- ❸ Click **Exclusions** to open the **Set Exclusions** dialog box.
- ❹ Add files, folders, or drives or edit an item in the list.
- ❺ To add an item, click **Add** to open the **Add Exclusion Item** dialog box.
- ❻ Under **What to exclude**, select the folder using **By name/location**.
- ❼ Under **When to exclude**, specify all options.
- ❽ Click **OK** to save these settings and return to the **Set Exclusions** dialog box.
- ❾ Click **OK** to save these settings and return to the **Detection** tab.
- ❿ Click **Apply** to save these settings.

MSDE installation problem

If an old release of MSDE (before Service Pack 3) is installed on Windows XP (Service Pack 2), there may be no errors during installation. However, due to some security vulnerability of older versions of MSDE, Windows disallows the SQL server to use port 1433. This results in disconnections to the database during IMS Server installation.

Use the Event Viewer in the Applications category to find the logs generated by SQL server. Older versions of MSDE should indicate that port 1433 cannot be used due to a vulnerability in the current version of MSDE.

To resolve this issue, apply MSDE 2000 Service Pack 3 (or a newer version), or just download the latest release of MSDE installer from the Microsoft website.

IMS Server installation problem due to database configuration

The IMS Server installation may fail if the database server has been configured to return **No Count**. Since the IMS Server uses these counts to determine the success or failure of database operations, this database feature must be disabled.

To disable the database feature:

- ❶ From Enterprise Manager, right-click on the database server and select **Properties**.
- ❷ Go to *Connection >> No Count*, and disable it.

The IMS Server installation may also fail if the database has incorrect user privileges. The database user should have public, db_owner rights for the IMS database. The user should not be a DB Administrator account.

To check whether the database user has the correct privileges:

- ❶ Click on *DB Server >> Security >> Logins*.
- ❷ Right-click on **DB login** and select **Properties**.
- ❸ Click on the **Server Roles** tab.
- ❹ Privileges are incorrect if the **System Administrators** and **Database Creators** roles are marked. If incorrect, manually prepare the IMS database and refer to the instructions in [Preparing the IMS database](#).

Failure to connect to named instance of SQL Server 2000 database

If an earlier version of IMS Server is upgraded to version 3.3.1.4 or above, the upgrade may fail if the IMS database is a named instance of an SQL Server 2000 database. The error message "There was a problem uploading all_storage_templates.xml" is displayed, since the IMS Server cannot connect to the database.

This problem is due to a bug in a Microsoft's SQL Server 2000 JDBC driver used prior to IMS Server version 3.3.1.4, which ignores the database port number field if a named instance is used.

In the new SQL Server 2005 JDBC driver used in IMS Server version 3.3.1.4 and above, the port number field is not ignored, and the database connection would fail if the port number is incorrect.

To fix this problem during an IMS Server upgrade, modify the IMS Server configuration file to correct the port number.

- Provide the correct port number in the following keys in the **ims.xml** file (found in **<IMS Installation Folder>\ims\config**): **ds.ims.rdb.uri** and **ds.ims_log.rdb.uri**.

For example, if the correct port number is 1074, replace
jdbc:microsoft:sqlserver://serverName\instanceName:1433 with
jdbc:microsoft:sqlserver://serverName\instanceName:1074.

- To find the port number that is running the instance, click *Start >> Programs >> Microsoft SQL Server >> Server Network Utility >> Choose TCP/IP >> Click Properties >> Right-click on database server and select Properties*.

For a fresh IMS Server installation, make sure that the port number in the installation wizard is correct.

Application does not work properly after AccessAgent is installed

Some Microsoft DLLs are used by AccessAgent when observing applications. If the DLL versions conflict with those used by an application, the application may not work properly.

To check for DLL conflicts:

- 1 Launch command prompt (*Start >> Run >> cmd*).

```
net stop obsservice
```

- 2 Launch the application and check if the application is working properly.

You can check the application folder to see if it is carrying any Microsoft DLLs, which are usually named **ms*.dll** (e.g., **msvcr70.dll**, **msvcp70.dll**).

A fix for the problem is to use the DLL redirection configuration suggested by Microsoft: <http://msdn2.microsoft.com/en-us/library/ms682600.aspx>.

Another possible fix is to replace the DLL carried by the application with a DLL compatible with AccessAgent. However, the application must also be compatible with the same DLL.

Cannot log on to Wallet after AccessAgent is installed

If you are using a version of AccessAgent before 3.3.1.4, there is a bug that prevents users from logging on if the machine Wallet is larger than 2MB. This can happen if there is a large number of AccessProfiles.

When attempting to log on, users will see the following error prompt: "You do not have a Wallet stored on this computer. However, you cannot download your Wallet from IMS Server because network connectivity is currently unavailable. Please try again later."

To resolve this problem, upgrade to AccessAgent version 3.3.1.4 or above. You can also reduce the number of AccessProfiles so the machine Wallet is less than 2MB in size.

Note that the inability to log on may also be due to any of the problems listed in [Unable to connect to the IMS Server](#).

Application is slower when automatic sign-on is enabled

Some applications may respond slower when automatic sign-on is enabled, or there may be a noticeable delay before credentials are auto-filled or auto-captured.

This may be due to the use of an inefficient XPath comparison in the AccessProfile for the affected application. If an XPath where **@title** is the only predicate checked for top level window (e.g., **/child::wnd[@title="Lagon"]**), AccessAgent will try to retrieve the title of each top level window using Windows messages.

However, for some applications, many hidden top level windows may be created during logon, and may take at least 0.5 seconds to respond to Windows messages. The response time in fetching the title of each window adds to the delay.

For such cases, use more specific XPaths reduce the number of matching windows. For example, the **@class_name** predicate can be used in the XPath to filter only windows of a certain class so that the title is fetched for fewer windows (fetching of class name does not require Windows messaging).

Missing labels in state engine view of AccessStudio

In some Windows 2000 machines, the state engine view of AccessStudio may show a graph with the states and connections without any labels. The names of the states, triggers, and actions appear to be missing. This is due to the Arial font not being supported on the machine. The workaround is to install the Arial font.

Spontaneous termination of sync.exe

Symptoms:

- ❶ After the first reboot, EnGINA does not show up. Instead, it bypasses to Microsoft GINA.
- ❷ Once logged on to Windows, the PC appears to be very slow. Stopping **ObsService** restores the computer to its original speed.
- ❸ **sync.exe** does not show up in Task Manager.
- ❹ After starting **sync.exe** manually, it shuts down within milliseconds.

Causes:

Anti-spyware, such as LanDesk software monitoring tool (**SoftMon.exe**) may have identified the process **sync.exe** to be a spyware/malware. The anti-spyware shuts down the process once it is detected. It appears in the AccessAgent logs as if **sync.exe** is crashing at different instances.

Resolution:

Add **sync.exe** to the LanDesk software monitoring tool's exclusion list. After making the settings, LanDesk ignores **sync.exe** and does not shut down the process. For other anti-spyware products, make the same changes to their exclusion lists.

GINA conflict with ThinkPad fingerprint software

Symptoms:

On a ThinkPad PC with a built-in fingerprint reader, EnGINA is not displayed during startup. Instead, the system crashes.

Causes:

The ThinkPad ThinkVantage fingerprint GINA (**vrlogin.dll**) conflicts with EnGINA.

Resolution:

Disable the ThinkVantage fingerprint GINA (*Start >> ThinkVantage fingerprint >> Control Center*) before installing AccessAgent. If AccessAgent is already installed, make sure that this registry entry is set to blank:

[HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate] "PrevGINA"

AccessAgent fails to install

If AccessAgent fails to install, check for the following:

- Windows Scripting Host 5.6 and above should be installed.
- WMI needs to be functional. To verify, go to *Computer Management >> Services and Applications >> WMI Control*. Right-click on **Properties** and see if the message "Successfully Connected to: <local computer>" is displayed. If no message is displayed, AccessAgent will not install.

Cannot log on to cached Wallets

If AccessAgent can log on when the IMS Server is online, but cannot log on to cached Wallets while the IMS Server is offline, the cached Wallets may be corrupted. For such cases, delete all cached user Wallets and try logging on again.

Enable the AccessAgent right-click option for **Delete user Wallets** by setting the machine policy **pid_wallet_delete_enabled** to **1**, which can be set through the registry entry **[HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\Temp]"WalletDeleteEnabled"**.



The menu item is only available when no one is logged on to AccessAgent. The user Wallets are deleted, not the machine Wallet. If this feature is used on a Citrix or Terminal Server or a workstation with Local User Session Management (LUSM) enabled, ensure that one (1) desktop session is running while deleting the Wallets. If multiple sessions are running, AccessAgent in other sessions may not function properly.

A message, "Microsoft SQL Server 2000 SP3a or above required" displayed when installing MOM 2005

Refer to Microsoft KB 902803: <http://support.microsoft.com/kb/902803/en-us?spid=2548>.

A message, "Failed to create data source for data warehouse" displayed when installing MOM Reporting

Refer to Microsoft KB 555533: <http://support.microsoft.com/default.aspx?scid=kb;en-us;555533>.

A message, "The MOM Server detected that DCOM was disabled on the remote computer" displayed when installing MOM Agent

To resolve the problem:

- ❶ Open **dcomcnfg** in *Start >> Run*.
- ❷ Go to *Console Root >> Component Services >> My Computer*.
- ❸ Right-click on **My Computer** and select **Properties**.
- ❹ In the *My Computer Properties* dialog, select **Default Properties** tab.
- ❺ Make sure the **Enable Distributed COM on this computer** option is marked.

Performance data is not available in MOM reports

To resolve the problem:

- ❶ Open the MOM Administrator console.
- ❷ Go to *Console Root >> Microsoft Operations Manager (SERVER_NAME) >> Administration >> Computers >> Agent-managed Computers*.
- ❸ Right-click on the computer with MOM agent installed, then select **Run Attribute Discovery Now**.

Definitions of policies

Policies can be modified only by Helpdesk officers and Administrators, because these policies affect the behavior of the whole system and should only be modified when it is absolutely necessary. These policies should be set at deployment and followed through.

Changes to these policies are propagated to clients the next time AccessAgent synchronizes with the IMS Server.

This appendix covers the following topics:

- [Setting policy priorities](#)
- [Legend](#)
- [Policies](#)

Setting policy priorities

If a policy is defined for two scopes (e.g: machine and system; user and system; machine and user), we need to define a priority in case the timeout value is different for one scope and the other.

For example, if the policy priority is "machine", then only the machine policy would be effective.

Policies can be modified only by Helpdesk officers and Administrators, because these policies affect the behavior of the whole system and should only be modified when it is absolutely necessary.

These policies should be set at deployment and followed through. Changes to these policies are propagated to clients the next time AccessAgent synchronizes with the IMS Server.

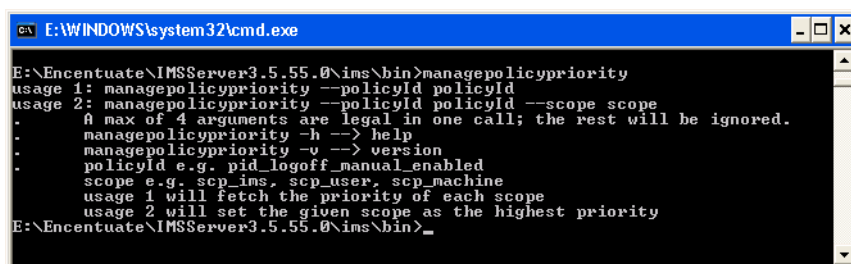
Use the **managepolicy.bat** Command Line Tool (CLT) to view and modify policy priorities. This CLT allows Administrators to retrieve the priority of a given policy, as well as set its priority by identifying a valid policy ID and scope.



Older versions of AccessAgent will still use the original policy priorities, and values will not change after IMS is upgraded. To change policy priorities, upgrade all installations of AccessAgent 3.6 and above, and then launch the command prompt.

To view the current priority of a policy:

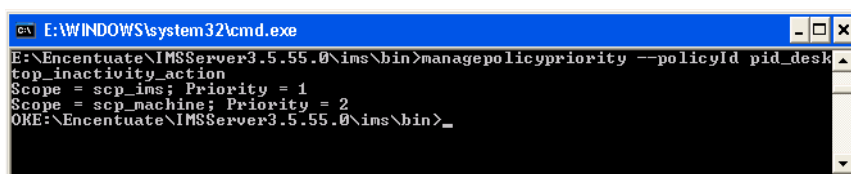
- 1 Click **Start >> Run** from your Windows Desktop. Enter **cmd** to launch the command prompt.
- 2 Navigate to the folder of the batch file by entering **cd\Encentuate\[IMS Server folder]\ims\bin**, then press **Enter**.
- 3 Enter **managepolicypriority** to view the information on executing the batch file, then press **Enter**. The details are displayed on the window.



```
E:\WINDOWS\system32\cmd.exe
E:\Encentuate\IMSServer3.5.55.0\ims\bin>managepolicypriority
usage 1: managepolicypriority --policyId policyId
usage 2: managepolicypriority --policyId policyId --scope scope
      A max of 4 arguments are legal in one call; the rest will be ignored.
.
.
managepolicypriority -h --> help
managepolicypriority -v --> version
policyId e.g. pid_logoff_manual_enabled
scope e.g. scp_ims, scp_user, scp_machine
usage 1 will fetch the priority of each scope
usage 2 will set the given scope as the highest priority
E:\Encentuate\IMSServer3.5.55.0\ims\bin>_
```

Executing the batch file

- 4 To view the scope and priority of a specific policy, enter **managepolicypriority -policyId [name of policy]**, then press **Enter**. The scope and priority of a policy is displayed.



```
E:\WINDOWS\system32\cmd.exe
E:\Encentuate\IMSServer3.5.55.0\ims\bin>managepolicypriority --policyId pid_desk
top_inactivity_action
Scope = scp_ims; Priority = 1
Scope = scp_machine; Priority = 2
OKE:\Encentuate\IMSServer3.5.55.0\ims\bin>_
```

Policy scope and priority

To set the priority of a policy:

- 1 Get the path from the folder of the batch file (**cd\Encentuate\[IMS Server folder]\ims\bin**), then press **Enter**.
- 2 To change the scope of the policy, enter **managepolicypriority --policyId [name of policy] --scope [scp_ims or scp_machine]**, then press **Enter**.


```

E:\Encentuate\IMSServer3.5.55.0\ims\bin>managepolicypriority --policyId pid_desk
top_inactivity_action
Scope = scp_ims; Priority = 1
Scope = scp_machine; Priority = 2
OKE:\Encentuate\IMSServer3.5.55.0\ims\bin>managepolicypriority --policyId pid_de
sktop_inactivity_action --scope scp_machine
OKE:\Encentuate\IMSServer3.5.55.0\ims\bin>_

```


Changing the policy scope

The scope that will be given first priority is assigned a value of "1", the next scope a value of "2", and so on.

- ③ Enter **exit** to close the command prompt.

Legend

Attribute	Description
Policy ID	Unique identifier of the policy.
Description	Description of the policy, including a list of the possible behaviors specified by the policy. The product version that implements this policy is also indicated.
Registry	<p>The entry in the Windows Registry (for Machine policies) or the IMS (for System, User, and Machine policies):</p> <ul style="list-style-type: none"> ■ [DO] is [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\DeploymentOptions] ■ [DIMS] is [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\IMSService\DefaultIMSSettings] ■ [GIMS] is [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\IMSService\GlobalIMSSettings] ■ [T] is [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\Temp]
IMS Entry	The entry in the IMS for System and User policies.

Attribute	Description
Values	<p>Possible values that the policy can take on.</p> <p>The default value is indicated with an asterisk "*". The default value is used if the policy is not specified or if the specified value is invalid.</p> <p>The refresh frequency is also indicated here. This indicates when a policy will take effect after it is changed.</p> <ul style="list-style-type: none"> ■ Refreshed on use: Policy read from IMS/registry every time it is used. Changes, for example, take effect immediately. ■ Refreshed on sync: Policy read from IMS/registry only on the next synchronization with IMS. ■ Refreshed on logon: Policy read from IMS/registry only on the next AccessAgent logon. ■ Refreshed on startup: Policy read from IMS/registry only on system startup.
Scope	<p>The scope of applicability of the policy.</p> <p>Values:</p> <ul style="list-style-type: none"> ■ System: Policy is system-wide ■ Machine: Policy affects only a specific machine ■ User: Policy affects only a specific user <p>System and User policies, as well as selected Machine policies can be configured using AccessAdmin. If pid_machine_policy_override_enabled is 1, machine policies can also be specified as Windows registry entries on individual machines, and they will override the ones defined via AccessAdmin.</p> <p>A policy may be defined for different scopes. For example, pid_desktop_inactivity_mins may define the desktop inactivity timeout duration for a machine or for a user. If this policy is defined for both scopes, we need to define a priority in case the timeout value is different for the machine and for the user. If policy priority is "machine", only the machine policy would be effective.</p>
	Frequently used policies

Policies

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

AccessAgent configuration

* pid_second_factors_supported_list

<p>The 2nd factors supported on this machine. Controls the Wallet registration policy. Also imposes a constraint on the Wallet locks available for login.</p> <p><i>Note: Should the user decide to switch second factors (e.g. from ARFID to RFID), a machine restart is required.</i></p>	<p>[DO]</p> <p>"SecondFactorsSupportedList"</p>	<p>Authentication second factors supported</p>	<p>#RFID</p> <p>#ARFID</p> <p>#USB</p> <p>#Fingerprint</p> <p>(currently, only single value allowed, except for simultaneous Fingerprint and RFID support)</p> <p>(refreshed on restart)</p>	<p>Machine</p>
--	---	--	--	----------------

pid_aa_tray_bubble_display_enabled

<p>Whether to enable Access Agent's bubble pop-ups at the Windows notification area.</p>	<p>[DO]</p> <p>"AATrayBubbleDisplayEnabled"</p>	<p>Enable bubble pop-ups?</p>	<p>*#True</p> <p>#False</p> <p>#0: No</p> <p>*#1: Yes</p> <p>(refreshed on use)</p>	<p>Machine</p>
--	---	-------------------------------	---	----------------

pid_aa_tray_menu_options_enabled

<p>Whether to display menu options when user right-clicks AccessAgent icon at the Windows notification area.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If policy value is 0, no menu is displayed when AccessAgent icon is right-clicked. 2. However, if the user double-clicks the AccessAgent icon, normal AccessAgent UI pops up and the user can click on the appropriate option on the AccessAgent UI. 	<p>[DO]</p> <p>"AATrayMenuOptionsEnabled"</p>	<p>Enable right-click menu options?</p>	<p>*#True</p> <p>#False</p> <p>#0: No</p> <p>*#1: Yes</p> <p>(refreshed on use)</p>	<p>Machine</p>
--	---	---	---	----------------

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

Network

Session Information

pid_session_info_display_freq_secs

<p>Frequency for displaying AccessAgent session information in a bubble pop-up at the Windows notification area. The bubble pops up after every interval, in seconds, specified by this policy. Disable this feature by setting it to 0.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <i>pid_aa_tray_bubble_display_enabled</i> is 1. 2. Set policy to 0 to disable the displaying of session information. 3. If the bubble pop-up will be constantly displayed (unless clicked by user), set this policy to a value less than or equal to <i>pid_session_info_display_dur_secs</i>. 4. The displayed user name format is determined by <i>pid_logon_user_name_display_option</i>. 5. If user is logged on with Active Proximity Badge, a warning is shown in the same bubble pop-up if battery is low. 	<p>[DO] "SessionInfoDisplayFreqSecs"</p>	<p>Interval, in minutes, for displaying session information in bubble pop-ups</p>	<p>*0 (refreshed on start-up) (0 for no display)</p>	<p>Machine</p>
---	--	---	--	----------------

Logs

pid_log_file_count

<p>Maximum number of AccessAgent log files allowed. Once the maximum number of log files is reached, the oldest log file is deleted to make way for the new log file.</p>	<p>[DO] "LogFileCount"</p>		<p>*10 (refreshed on use)</p>	<p>Machine</p>
---	--------------------------------	--	-----------------------------------	----------------

pid_log_file_size

<p>Maximum size, in KB, of the log file ("AccessAgent.log"). Once the maximum size is reached, the file is renamed and a new file will be created to store the new logs.</p>	<p>[DO] "LogFileSize"</p>		<p>*1024 (refreshed on use)</p>	<p>Machine</p>
--	-------------------------------	--	-------------------------------------	----------------

Description	Registry	IMS Entry	Values	Scope
pid_log_level				
Level of log details.	[DO] "LogLevel"		*#0: No logging #1: Severe errors only #2: Basic info #3: More info, including SOAP logs #4: Debugging info, including SOAP logs (refreshed on use)	Machine
pid_log_path				
Path to a folder that contains the AccessAgent logs.	[DO] "LogPath"		*<Program-Dir>\logs (refreshed on use)	Machine

Temporary files

pid_temp_path				
Path to a folder that contains the temporary files.	[DO] "TempPath"		*<Program-Dir>\temp (refreshed on use)	Machine

Auto-logon

pid_microsoft_auto_logon_enabled				
Whether to enable auto-logon to Windows on system startup.	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon] "AutoAdminLogon" "ForceAutoLogon" (both entries must be set)		*#0: No #1: Yes (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_microsoft_auto_logon_acct				
Windows account to be used for auto-logon on system startup. <i>Notes:</i> 1. Effective only if <i>pid_microsoft_auto_logon_enabled</i> is enabled. 2. If <i>pid_lusm_session_max</i> > 1, a local machine account should be used for auto-logon.	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon] "DefaultDomainName" "DefaultUserName" "DefaultPassword"		(refreshed on use)	Machine


* pid_win_startup_action

Actions on Windows startup. <i>Note: This is to enable automatic locking of computer after AutoAdminLogon or ForceAutoLogon.</i>	[DO] "WinStartupAction"	Windows startup actions	*#0: No action *#1: Lock computer (refreshed on use)	Machine
---	----------------------------	-------------------------	--	---------

Local user session management policies

pid_lusm_session_replacement_option

Option for replacing existing user sessions when a new user attempts to log on while the number of concurrent user sessions has already reached the maximum allowed. <i>Notes:</i> 1. Effective only if <i>pid_lusm_sessions_max</i> > 1. 2. Policy value 2 is useful for machines which are used by users in a round-robin fashion. 3. For policy value 3, the session that has been unlocked the least number of times will be replaced. 4. For policy value 4, the session that has been least used in terms of total duration will be replaced. 5. Computation of time for all cases is accurate only to the nearest minute.	[DO] "LUSMSessionReplacementOption"	Session replacement option	#0: Disallow new user to log on *#1: Replace least recently used (LRU) session #2: Replace most recently used (MRU) session #3: Replace least frequently used (LFU) session #4: Replace least used (LU) session (refreshed on startup)	Machine
--	--	----------------------------	---	---------

Description	Registry	IMS Entry	Values	Scope
 pid_lusm_sessions_max				
<p>Maximum number of concurrent user sessions. Set it to 2 or more to enable private desktop.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Set policy to 1 to disable Local User Session Management. 2. To enable Local User Session Management, a value greater than 1 should be specified for this policy in the <i>DeploymentOptions.reg</i> file during AA installation. If this policy is set to a value greater than 1 only after AA is installed, the "Log Off" and "Shut Down" buttons, as well as the Windows hot keys may not be disabled for the very first user who logs on. Also, the buttons and Windows hot keys may remain disabled after AA is uninstalled. 3. If this policy is set to a value higher than what the system resources can support, the actual number of concurrent user sessions will still be capped by the system resources available. 4. For optimal performance, it should not be set to a value more than 9 (RAM should be more than 1GB). 5. If Local User Session Management is enabled, <i>pid_logoff_manual_action</i> should be set to 1 (Log off Windows) so that manually logging off AA will be equivalent to logging off the user's desktop session. <p><i>pid_unlock_with_win_option</i> should be set to 0 as unlock using Windows is not supported for Local User Session Management. Auto admin logon to Windows should also be enabled by setting <i>pid_microsoft_auto_logon_enabled</i> to 1, <i>pid_microsoft_auto_logon_acct</i> to a local machine logon account, and <i>pid_win_startup_action</i> to 1, so as to lock the computer immediately after logon.</p>	<p>[DO] "LUSMSessions- Max"</p>	<p>Maximum number of concurrent user sessions on a workstation</p>	<p>*1 (refreshed on startup) (from 1 to 12)</p>	<p>Machine</p>

Description	Registry	IMS Entry	Values	Scope
pid_lusm_sia_list				
<p>List of single instance applications (SIA), such as applications that cannot run multiple simultaneous instances in a computer.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <code>pid_lusm_sessions_max > 1</code>. 2. When a user starts any application in this list, AccessAgent performs the action specified by <code>pid_lusm_sia_launch_option</code> (if the policy value is not 0) or application's own launch option. Note that these actions are only applicable when the application is launched from a visible desktop and there is another instance of it running in an invisible desktop. If the other instance is running in the same visible desktop, the application will assume its normal behavior. 3. For each application, the full path should be the full image path of the executable on the disk, ending with ".exe", ".bat", or ".com". It is case-insensitive. 4. Note that the long path format should be used. For example, for Yahoo Messenger, use "C:\Program Files\Yahoo!\Messenger\YahooMessenger.exe" instead of "C:\program~1\Yahoo!\messenger\YAHOOM~1.exe". 	<p>[DO] "LUSMSiaList"</p>	<p>Single instance applications list</p>	<p>Each application occupies 3 lines as follows:</p> <p>Line 1: Full path of executable (e.g., C:\Windows\notepad.exe)</p> <p>Line 2: Launch option (see below)</p> <p>Line 3: Display name of the application (e.g., Notepad)</p> <p>(empty lines are discarded, and hence, there must be 3 non-empty lines for each application)</p> <p>Launch option is one of the following values:</p> <p>#1: Disallow 2nd instance to start</p> <p>*#2: Log off existing instance</p> <p>#3: Close existing instance</p> <p>#4: Prompt user whether to log off existing instance</p> <p>#5: Prompt user whether to close existing instance (refreshed on startup)</p>	<p>Machine</p>

Description	Registry	IMS Entry	Values	Scope
pid_lusm_sia_launch_option				
<p>Action taken by AccessAgent when user launches a 2nd instance of a single instance application, such as an application that cannot run multiple simultaneous instances in a computer.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <code>pid_lusm_sessions_max > 1</code>. 2. If policy value is 0, the each application's own launch option (specified in <code>pid_lusm_sia_list</code>) is used. 3. Note that these actions are only applicable when the application is launched from a visible desktop and there is another instance of it running in an invisible desktop. If the other instance is running in the same visible desktop, the application will assume its normal behavior. 	<p>[DO]</p> <p>"LUSMSiaLaunchOption"</p>	<p>Action on launching a second instance of a single instance application</p>	<p>#0: Use application's launch option</p> <p>#1: Disallow 2nd instance to start</p> <p>*#2: Log off existing instance</p> <p>#3: Close existing instance</p> <p>#4: Prompt user whether to log off existing instance</p> <p>#5: Prompt user whether to close existing instance (refreshed on startup)</p>	Machine
pid_lusm_generic_accounts_enabled				
<p>Whether to use a pool of generic accounts to create user desktops.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <code>pid_lusm_sessions_max > 1</code>. 2. If enabled, generic accounts specified in <code>pid_lusm_generic_accounts_list</code> will be used to create user desktops. This configuration is for deployments where some Encentuate users may not exist in AD, or Encentuate password is not synchronized with AD password. 3. If enabled, <code>pid_lusm_default_desktop_preserved_enabled</code> must be set to 1. 	<p>[DO]</p> <p>"LUSMGenericAccountsEnabled"</p>	<p>Enable use of generic accounts to create user desktops?</p>	<p>#True</p> <p>*#False</p> <p>*#0: No</p> <p>#1: Yes (refreshed on startup)</p>	Machine

Description	Registry	IMS Entry	Values	Scope
pid_lusm_generic_accounts_list				
<p>List of generic accounts for creating user desktops.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <code>pid_lusm_sessions_max > 1</code> and <code>pid_lusm_generic_accounts_enabled</code> is enabled. 2. Upon machine start-up, <code>AccessAgent</code> writes the obfuscated password into the 4th line of each account, replacing the 3rd line with a fixed mask string <code>"#####encrypted#####"</code>. 3. To add a new account, delete an existing account, or change the user name, domain, or password of an existing account, the entire set of values in this policy must be re-written. <code>AccessAgent</code> will use the new values after the next machine start-up. 4. If a particular account cannot be validated, this account will be ignored and <code>AccessAgent</code> will write <code>"#####invalid account#####"</code> in the 3rd line of the account. 5. If the number of valid accounts is less than two, the generic accounts feature will be disabled. 6. If the number of valid accounts is less than <code>pid_lusm_sessions_max</code>, the actual maximum number of concurrent sessions would be constrained by the number of valid accounts even though resources may allow for more. 7. Both local machine accounts or domain accounts can be used as generic accounts, but domain accounts are recommended since these accounts do not have to be pre-created on each machine. However, note that the passwords for these accounts should never expire nor be changed, since any password changes will require modifications to this policy. 8. Users should not unlock directly using generic account credentials as that may lead to an existing user's desktop being unlocked. 	<p>[DO]</p> <p>"LUSMGenericAccountsList"</p>		<p>Each generic account occupies 4 lines as follows:</p> <p>Line 1: User name</p> <p>Line 2: Domain (or machine name for local computer account)</p> <p>Line 3: Password</p> <p>Line 4: ==</p> <p>(empty lines are discarded, and hence, there must be 4 non-empty lines for each account)</p> <p>(refreshed on start-up)</p>	Machine

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

Authentication policies

* pid_wallet_authentication_option

<p>Authentication policy that enforces the combinations of authentication factors that can be used for logon.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This policy does not enforce authentication factors to be used for sign-up. Sign-up policy is enforced by <code>pid_second_factors_supported_list</code> and <code>pid_second_factor_for_sign_up_required</code> 2. RFID includes active proximity badges. 		<p>Wallet authentication policy</p>	<p>#1: Password</p> <p>#2: Password + RFID</p> <p>*#3: USB Key</p> <p>#5: Fingerprint (multiple allowed)</p> <p>(refreshed on logon or unlock by different user, if online)</p> <p>(refreshed on last sync if offline)</p> <p>Note: #3 is always enabled. #1 enabled => #2 is also enabled.</p>	User
--	--	-------------------------------------	--	------

* pid_mac_auth_enabled

<p>Whether Mobile ActiveCode authentication is enabled for the user.</p>		<p>Enable Mobile ActiveCode authentication?</p>	<p>#True</p> <p>*#False (refreshed on use)</p>	User
--	--	---	--	------

Encentuate password policies

pid_enc_pwd_is_usb_key_pwd_enabled

<p>Whether to set Encentuate password to last changed USB Key password.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If enabled, Password authenticator's password will always be set to be the same as the USB Key password when the latter is changed. 2. This policy should be enabled for normal users and disabled for power users. 		<p>Set Encentuate password to last changed USB Key password?</p>	<p>*#True</p> <p>#False (refreshed on next successful password change)</p>	User
---	--	--	--	------

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

Encentuate password aging policies

pid_enc_pwd_periodic_change_enabled				
Whether to enable password aging, such as periodic password change.		Enable password aging?	#True *#False (refreshed on sync)	System

pid_enc_pwd_change_days				
Maximum password age, in days. It is the period, in days, between two password changes for a Wallet or USB Key. <i>Note: Effective only if Encentuate password periodic change is enabled.</i>		Maximum password age, in days	*90 (refreshed on sync)	System

pid_enc_pwd_expiry_reminder_enabled				
Whether to remind user about expiring password. <i>Note: Effective only if Encentuate password periodic change is enabled.</i>		Enable password change reminder?	#True *#False (refreshed on sync)	System

pid_enc_pwd_expiry_reminder_days				
Number of days before password expiry to start reminding user. <i>Note: Effective only if Encentuate password expiry reminder is enabled.</i>		Number of days before password expiry to start reminding user	*5 (from 1 to 10) (refreshed on sync)	System

pid_enc_pwd_expiry_change_enforced				
Whether to enforce password change on expiry by prompting user to change password before logging on to AccessAgent. <i>Note: Effective only if Encentuate password periodic change is enabled.</i>		Enforce password change on expiry?	#True *#False (refreshed on sync)	System

Encentuate password strength policies

pid_enc_pwd_min_length				
Minimum length of an acceptable Encentuate password. <i>Note: Not effective if Encentuate password is AD password is enabled. AD password strength policies will be used instead.</i>		Minimum password length	*6 (from 1 to 99) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_enc_pwd_max_length				
Maximum length of an acceptable Encentuate password. <i>Note: Not effective if Encentuate password is AD password is enabled. AD password strength policies will be used instead.</i>		Maximum password length	*20 (from 1 to 99) (refreshed on sync)	System
pid_enc_pwd_min_numerics_length				
Minimum number of numeric characters for an acceptable Encentuate password. <i>Note: Not effective if Encentuate password is AD password is enabled. AD password strength policies will be used instead.</i>		Minimum number of numeric characters	*0 (from 0 to 99) (refreshed on sync)	System
pid_enc_pwd_min_alphabets_length				
Minimum number of alphabetic characters for an acceptable Encentuate password. <i>Note: Not effective if Encentuate password is AD password is enabled. AD password strength policies will be used instead.</i>		Minimum number of alphabetic characters	*0 (from 0 to 99) (refreshed on sync)	System
pid_enc_pwd_mixed_case_enforced				
Whether to enforce the use of both upper case and lower case characters for the Encentuate password. <i>Note: Not effective if Encentuate password is AD password is enabled. AD password strength policies will be used instead.</i>		Enforce the use of both upper case and lower case characters?	#True *#False (refreshed on sync)	System

Self-service password reset policies

* pid_selfhelp_password_reset_enabled

Whether to enable self-service password reset.		Enable self-service password reset?	#True *#False (refreshed on sync)	System
pid_secrets_register_for_selfhelp_max				
The maximum number of secret questions a user should register to enable self-service capability.		Maximum number of secret questions a user should register to enable self-service	*3 (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_secrets_verify_for_selfhelp				
The number of secret questions a user needs to answer for using self-service.		The number of secret questions a user needs to answer to use self-service.	*2 (refreshed on sync)	System

pid_secrets_verify_invalid_trial_count_max				
The maximum number of invalid tries allowed before self-service capability gets locked.		The maximum number of invalid tries allowed before self-service locks out	*6 (refreshed on sync)	System

Self-service authorization code policies

pid_selfhelp_authcode_enabled				
Whether to enable self-service authorization code issuance using mobile phone.		Enable self-service authorization code issuance?	#True *#False (refreshed on use)	System

pid_selfhelp_authcode_request_from_any_phone_enabled				
Whether to allow self-service authorization code to be requested from any phone. <i>Note: Effective only if pid_selfhelp_authcode_enabled is True.</i>		Allow authorization code request from any phone?	#True *#False (refreshed on use)	System

pid_selfhelp_authcode_invalid_trial_count_max				
The maximum number of invalid trials allowed before self-service authorization code request capability gets locked. <i>Note: Effective only if pid_selfhelp_authcode_enabled is True.</i>		The maximum number of invalid tries allowed before self-service authorization code request locks out	*6 (refreshed on use)	System

pid_selfhelp_authcode_error_msg_text				
Configurable error message text for self-help authorization code request. <i>Note: Effective only if pid_selfhelp_authcode_enabled is True.</i>		Error message text for self-help authorization code request	*An error has occurred. Please contact your Helpdesk. (refreshed on use)	System

Description	Registry	IMS Entry	Values	Scope
pid_selfhelp_authcode_request_help_text				
<p>Configurable help text for self-service authorization code request.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <i>pid_selfhelp_authcode_enabled</i> is <i>True</i>. 2. The help text can be sent to user by the SMS gateway's IMS Bridge, shown by AccessAgent, etc. 		Help text for self-service authorization code request	*You can only request for authorization code using your registered phone. The message format is: User-Name UserSecret [RequestCode] (refreshed on use)	System
pid_selfhelp_authcode_issue_msg_text				
<p>Configurable message text for self-help authorization code issuance.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <i>pid_selfhelp_authcode_enabled</i> is <i>True</i>. 2. Use \$AUTHCODE as place-holder for authorization code. 3. Use \$VALIDITY as place-holder for no. of days for which authorization code is valid. 4. Use \$USAGE as place-holder for string that describes how the authorization code can be used. 		Message text for self-help authorization code issuance	*Your authorization code is \$AUTH-CODE. You can use it within \$VALIDITY days for \$USAGE. (refreshed on use)	System
pid_selfhelp_authcode_different_phone_error_msg_text				
<p>Configurable message text to be sent to requesting phone for self-help authorization code if it is different from registered phone and policy is such that only the registered phone can be used.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <i>pid_selfhelp_authcode_enabled</i> is <i>True</i> and <i>pid_selfhelp_authcode_request_from_any_phone_enabled</i> is <i>False</i>. 2. Use \$PHONE as place-holder for registered phone number. 		Message text sent to requesting phone if it is different from registered phone and only registered phone can be used	*Authorization code can only be requested from your registered phone \$PHONE. (refreshed on use)	System

Description	Registry	IMS Entry	Values	Scope
pid_selfhelp_authcode_different_phone_issue_msg_text				
Configurable message text to be sent to requesting phone for self-help authorization code if it is different from registered phone. Notes: 1. <i>Effective only if set to True in pid_selfhelp_authcode_enabled.</i> 2. <i>Use \$PHONE as place-holder for registered phone number.</i>		Message text sent to requesting phone if it is different from registered phone	*An authorization code has been sent to your registered phone \$PHONE. (refreshed on use)	System
pid_selfhelp_authcode_wrong_credentials_error_msg_text				
Configurable message text to be sent to requesting phone for self-help authorization code if any of the requesting credentials is incorrect. Notes: 1. <i>Effective only if set to True in pid_selfhelp_authcode_enabled.</i> 2. <i>Message text is sent if any of the requesting credentials is incorrect, for example, user name, user secret, request code.</i>		Message text sent to requesting phone on incorrect credentials	*Incorrect user name, user secret, or request code. Please try again. (refreshed on use)	System

Self-service registration and bypass of 2nd factor policies

pid_selfhelp_second_factor_registration_and_bypass_enabled

Whether to enable self-service registration and bypass of 2nd factor. Notes: 1. <i>If this policy is enabled, user can bypass the use of 2nd factor for logon by providing registered secrets instead.</i> 2. <i>Whether authorization code is required for registration of 2nd factors depends on pid_second_factor_registration_option. In cases where authorization code is required, this policy controls whether user can perform the action in a self-service manner by providing registered secrets instead.</i> 3. <i>If user is not able to provide registered secrets, there is an option to provide an authorization code and primary secret.</i> 4. <i>Registration of second factors using self-service secrets is not supported for USB Keys.</i>		Enable self-service registration and bypass of 2nd factor?	#True *#False (refreshed on sync)	System
--	--	--	---	--------

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

Wallet policies

pid_wallet_caching_option				
<p>Option to control the caching of Wallets.</p> <p><i>Note: Offline reset capability (f.k.a. BSK) is automatically enabled if Wallet is cached.</i></p>		Wallet caching option	#0: Disallow caching *#1: Ask user #2: Always cache (refreshed on sync)	System

pid_wallet_cache_max				
<p>Maximum number of cached Wallets allowed on the machine.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If the maximum limit has reached, the least recently used cached Wallet will be deleted before a new Wallet is cached. 2. Setting a limit on the number of cached Wallets for a shared workstation may improve logon performance. 3. If biometric authentication is used on a shared workstation, it is recommended that the limit on the number of cached Wallets be set to a value such that the possibility of false acceptance for the biometric device is made negligible. This is because false acceptance may lead to a user logging on to a wrong Wallet. 4. This policy should be used in conjunction with <code>pid_wallet_cache_max_inactivity_days</code> so that deleted cached Wallets can also be automatically revoked on the IMS Server. 5. In some deployments, it may be desirable to disable Wallet caching on shared workstations due to security reasons. This policy can be set to 0 to disable caching on a particular machine. In this case, it overrides <code>pid_wallet_caching_option</code>. 	[DO] "WalletCache-Max"	Maximum number of cached Wallets	*999999999 (0 to disable caching) (999999999 for no max limit) (refreshed on use)	Machine

pid_wallet_sync_mins				
<p>Interval, in minutes, for periodic synchronization of Wallet with IMS Server. Synchronization is also performed when user logs on to AccessAgent.</p>		Interval, in minutes, for synchronization of Wallet with IMS Server	*30 (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

pid_wallet_cache_max_inactivity_days				
<p>Maximum period of inactivity, in days, allowed for a cached Wallet. After which, the cached Wallet is automatically revoked.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If a cached Wallet is not used for a period exceeding the limit imposed by this policy, it is automatically revoked on the IMS Server. AccessAgent will also automatically revoke the cached Wallet when a user attempts to log on to it. 2. Inactivity is measured from the last synchronization time. Hence, even if a user logs on to a cached Wallet every day, it can still be revoked if it has not been synchronized with the IMS Server for an extended period of time. 3. If a cached Wallet is revoked, user will only be able to log on if IMS Server is available. There should be no prompt that the Wallet has been revoked, but the option to cache the Wallet may be given (depends on pid_wallet_caching_option). 		Maximum period of inactivity, in days, allowed for a cached Wallet	<p>*999999999</p> <p>(999999999 for infinity, such as cached Wallets do not expire)</p> <p>(refreshed on sync)</p>	System

pid_wallet_sync_before_logon_enabled				
<p>Whether to enable AccessAgent to perform synchronization with IMS Server before logging on to the Wallet.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If this policy is set to 1, AccessAgent performs synchronization before logging on through Windows logon (for EnGINA logon), and before running logon script (for desktop logon and logon from unlock screen). 2. Due to the longer time needed for USB Key to perform synchronization with IMS Server, this policy is recommended to be set to 0 for USB Key deployments. 	[DO] "WalletSyncBeforeLogonEnabled"	Enable Wallet synchronization before logon?	<p>*#True</p> <p>#False</p> <p>#0: No</p> <p>*#1: Yes</p> <p>(refreshed on use)</p>	Machine

pid_wallet_open_max_tries				
<p>Maximum number of consecutive invalid offline logons before cached Wallet is locked out.</p> <p>Note: This policy does not support Charismathics USB Keys.</p>		Maximum number of consecutive invalid offline logons before cached Wallet is locked out	<p>*5</p> <p>(refreshed on sync)</p>	System

Description	Registry	IMS Entry	Values	Scope
pid_wallet_editable_items_list				
List of Wallet items that can be edited by the user through AccessAgent.		List of Wallet items that can be edited by the user through AccessAgent.	*#1: Password *#2: Password entry option *#4: Application settings *#8: Delete credential *#16: Add credential (multiple allowed) (refreshed on sync)	User
pid_wallet_inject_pwd_entry_option_default				
Default automatic sign-on password entry option.		Default automatic sign-on password entry option	#1: Automatic logon *#2: Always #3: Ask #4: Never #5: Certificate #6: Use application settings (refreshed on sync)	System
pid_wallet_enterprise_app_never_option_enabled				
Whether the "Never" password entry option is enabled for enterprise authentication services. <i>Note: User policy, if defined, overrides system policy.</i>		Enable 'Never' for enterprise authentication services?	*#True #False (refreshed on sync)	User System
pid_wallet_personal_app_sso_enabled				
Whether to enable automatic sign-on for personal authentication services. <i>Note: User policy, if defined, overrides system policy.</i>		Enable automatic sign-on for personal authentication services?	*#True #False (refreshed on use for user policy) (refreshed on sync for system policy)	User System
pid_sso_auto_learn_enabled				
Whether auto-learning should be enabled for automatic sign-on to applications.		Enable auto-learning?	*#True #False (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_sso_user_control_enabled				
<p>Whether to allow user to enable/disable automatic sign-on.</p> <p><i>Note: If this policy is disabled, the "Enable automatic sign-on" and "Disable automatic sign-on" options will not appear in any part of AccessAgent UI.</i></p>	<p>[DO] "SsoUserControlEnabled"</p>	<p>Allow user to enable/disable automatic sign-on?</p>	<p>#0: No *#1: Yes *#True #False (refreshed on sync)</p>	<p>Machine User</p>
pid_accessagent_pwd_display_option				
<p>Option for displaying of application passwords in the Wallet Manager of AccessAgent through the "Show password" option.</p> <p><i>Notes:</i></p> <ol style="list-style-type: none"> 1. User is asked to enter Encentuate password before being allowed to display passwords. 2. Displaying of passwords is not allowed if user is logged on using fingerprint. 		<p>Option for displaying of application passwords in AccessAgent Non-negative integer</p>	<p>*#0: Disallow displaying passwords #1: Allow displaying personal passwords #2: Allow displaying both enterprise and personal passwords (refreshed on sync)</p>	<p>User</p>
pid_accessagent_pwd_export_option				
<p>Option for displaying of application passwords in the Wallet Manager of AccessAgent through the "Show password" option.</p> <p><i>Note: User is asked to enter Encentuate password before being allowed to display passwords.</i></p>		<p>Option for displaying of application passwords in AccessAgent</p>	<p>#0: Disallow displaying passwords #1: Allow displaying personal passwords *#2: Allow displaying both enterprise and personal passwords (refreshed on sync)</p>	<p>User</p>

Description	Registry	IMS Entry	Values	Scope
pid_migration_stage				
<p>Whether migration from IAM version 1.x to 3.x is in progress and, if so, the current stage of migration.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. The migration involves the upgrade of IMS Server, AccessAgent, and users' Wallets. 2. When IMS Server is upgraded, the installer automatically sets the policy value to 1. 3. This policy should be manually set by Administrator to 2 when all AccessAgent installations have been upgraded. 4. Users' Wallets are upgraded as and when they log on using upgraded AccessAgent. After all Wallets are upgraded, the policy should be set to 0 so as to optimize IMS Server and AccessAgent performance. <p>This can be done automatically by a nightly job that checks whether all Wallets have been upgraded.</p>		<p>Stage of migration from version 1.x to 3.x</p>	<p>*#0: No migration or migration completed</p> <p>#1: Upgrading IMS Server and AccessAgent</p> <p>#2: IMS Server and AccessAgent fully upgraded (refreshed on sync)</p>	System

Sign-up policies

pid_bind_secret_question_list				
<p>The set of questions that user will choose from during sign-up to provide the secret answer.</p>		<p>Question set for secret</p>	<p>*#What is your mother's maiden name?</p> <p>*#When is your birthday?</p> <p>(multiple allowed)</p> <p>(refreshed on sync)</p>	System
pid_secret_answer_min_length				
<p>Minimum length of an acceptable secret answer.</p>		<p>Minimum length of an acceptable secret answer</p>	<p>*3</p> <p>(refreshed on sync)</p>	System
pid_secrets_register_for_selfhelp_at_sign_up				
<p>Whether to prompt user to register additional secrets for self-service during sign-up.</p>		<p>Prompt user to register additional secrets for self-service during sign-up?</p>	<p>#True</p> <p>*#False</p> <p>(refreshed on sync)</p> <p>#False</p>	System

Description	Registry	IMS Entry	Values	Scope
pid_secret_option				
<p>Whether the secret is required, should be specified by user during sign-up, or automatically specified using a bind task.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This policy applies to users who are signing up or who are logging on for the first time after their accounts have been pre-provisioned. 2. For policy value 0, user would be assigned a system-defined secret. User would not be prompted for secret when performing actions that require it, for example, reset password, and offline recovery. Customer should understand the security vulnerabilities before deciding to implement such a configuration. 3. Currently, if policy value is changed from 1 to 0, users will be automatically migrated to system-defined secret when they log on to AccessAgent. However, there is no support for migration from policy value 0 to 1. 		Option for specifying secret	<p>#0: Secret not required</p> <p>*#1: Secret required, and user must specify during sign-up (refreshed on sync)</p>	System
pid_second_factor_for_sign_up_required				
<p>Whether 2nd factor is required during sign-up.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if second factors supported list is not empty, in which case, any one of the supported 2nd factors can be used for sign-up. There will be one UI dialog asking for user to present any one of the supported 2nd factors. 2. If policy value is 1, sign-up fails if 2nd factor is not presented. 	[DO] "SecondFactor-ForSignUpRequired"	Require authentication second factor during sign-up?	<p>#True</p> <p>*#False</p> <p>*#0: Not required</p> <p>#1: Required (refreshed on use)</p>	Machine

Description	Registry	IMS Entry	Values	Scope
* pid_automatic_sign_up_enabled				
<p>Whether to enable automatic sign up.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This policy should be set to 1 if Encentuate password is synchronized with Active Directory password. 2. pid_engina_welcome_text and pid_unlock_text should be modified accordingly if this policy is set to 1. 3. If this policy is set to 1, the "Sign up" option will not be available on both the AccessAgent UI and AccessAgent Tray menu; user will not be prompted to sign up if attempting to log on to an unregistered user name; user will not be prompted to confirm having signed up if an unregistered 2nd factor is presented. 	[DO] "AutomaticSign-UpEnabled"	Enable automatic sign-up?	#True *#False *#0: No #1: Yes (refreshed on use)	Machine

Policy templates

pid_policy_template_default

The default user policy template to be applied.		Default policy template	*default user policy template (refreshed on use)	System
---	--	-------------------------	---	--------

pid_machine_policy_template_default

The default machine policy template to be applied.		Default machine policy template	*default machine policy template (refreshed on use)	System
--	--	---------------------------------	--	--------

ActiveCode policies

pid_mac_max_validity_count

Maximum number of Mobile Active-Codes that may be valid for a user at any time.		Maximum number of Mobile Active Codes that may be valid for a user at any time.	*3 (from 1 to 7) (refreshed on use)	System
---	--	---	---	--------

Description	Registry	IMS Entry	Values	Scope
pid_activecode_bypass_option				
<p>Option for ActiveCode authentication bypass.</p> <p><i>Note: Can be used for bypassing both Mobile ActiveCode and OTP Active-Code (AccessAgent-OTP and on-board OTP).</i></p>		ActiveCode bypass option	<p>#1: Authorization code and Encentuate password</p> <p>#2: Authorization code and enterprise account password</p> <p>#4: Authorization code and secret (multiple allowed) (0 for "No bypass") (refreshed on use)</p>	System
pid_activecode_append_secret_option				
<p>Option for appending a secret to Mobile ActiveCode.</p> <p><i>Note: Please note that the order is also specified in the policy values.</i></p>		Option for appending a secret to Mobile Active-Code	<p>*#0: MAC only (no appending of secret)</p> <p>#1: MAC + Encentuate password</p> <p>#2: MAC + Enterprise account password</p> <p>#3: MAC + Administrator-assigned secret</p> <p>#4: Encentuate password + MAC</p> <p>#5: Enterprise account password + MAC</p> <p>#6: Administrator-assigned secret + MAC (refreshed on use)</p>	System

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

pid_otp_append_secret_option				
<p>Option for appending a secret to OTP (time-based) and OTP (OATH).</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Not applicable to AA-OTP and USB Key on-board OTP. 2. Please note that the order is also specified in the policy values. 		<p>Option for appending a secret to OTP (time-based) and OTP (OATH)</p>	<p>*#0: OTP only (no appending of secret)</p> <p>#1: OTP + Encentuate password</p> <p>#2: OTP + Enterprise account password</p> <p>#3: OTP + Administrator-assigned secret</p> <p>#4: Encentuate password + OTP</p> <p>#5: Enterprise account password + OTP</p> <p>#6: Administrator-assigned secret + OTP</p> <p>(refreshed on use)</p>	System

pid_otp_reset_sample_count				
<p>Number of consecutive OTPs to be obtained from user for resetting an OTP (OATH) token.</p>		<p>Number of consecutive OTPs needed for resetting an OTP (OATH) token</p>	<p>*3</p> <p>(from 1 to 5)</p> <p>(refreshed on sync)</p>	System

pid_activecode_admin_assigned_secret_name				
<p>Identity attribute name of the Administrator-assigned secret, for appending to ActiveCode.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Can be used for both Mobile ActiveCode and OTP ActiveCode (AccessAgent-OTP and on-board OTP). 2. Effective only if ActiveCode append secret option is 3. 		<p>Identity attribute name of the Administrator-assigned secret</p>	<p>(refreshed on use)</p>	System

AccessAssistant and Web Workplace policies

pid_accessanywhere_enabled				
<p>Whether user is allowed to use AccessAssistant.</p>		<p>Allow access to Wallet from AccessAssistant?</p>	<p>*#True</p> <p>#False</p> <p>(refreshed on use)</p>	User

Description	Registry	IMS Entry	Values	Scope
* pid_accessanywhere_second_factor_enabled				
Whether user is required to authenticate using second factor when using AccessAssistant.		Second factor authentication required for AccessAssistant?	*#True #False (refreshed on use)	User
pid_accessanywhere_personal_app_enabled				
Whether to display personal authentication services in AccessAssistant and Web Workplace. <i>Note: Effective only if pid_accessanywhere_enabled is True.</i>		Display personal authentication services in AccessAssistant and Web Workplace?	#True *#False (refreshed on sync)	User
pid_accessanywhere_edit_user_profile_enabled				
Whether the user profile can be edited by user in AccessAssistant and Web Workplace.		Enable editing of user profile in AccessAssistant and Web Workplace?	#True *#False (refreshed on sync)	System
pid_accessanywhere_second_factor_default				
The user's default second authentication factor for logging on to AccessAssistant and Web Workplace. <i>Notes:</i> 1. <i>Effective only if pid_accessanywhere_enabled and pid_accessanywhere_second_factor_enabled are True.</i> 2. <i>After user name and password are entered, AccessAssistant or Web Workplace will prompt for the default 2nd factor. User can still click on links to use other 2nd factors.</i> 3. <i>If the default 2nd factor is MAC, a MAC will automatically be sent to the user via the preferred channel right after entering user name and password. There will be a message indicating where the MAC has been sent to, and links for the user to request for MAC to be sent to another channel.</i> User should be able to change preferred MAC channel through the user profile settings page.		Default second authentication factor for AccessAssistant and Web Workplace	*#1: Authorization code #2: MAC #3: OTP (time-based) (refreshed on use)	User

Description	Registry	IMS Entry	Values	Scope
pid_accessanywhere_app_sso_enabled				
Whether the user can perform automatic sign-on to applications through AccessAssistant.		Enable automatic sign-on to applications in AccessAssistant?	#True *#False (refreshed on sync)	System
pid_accessanywhere_password_display_option				
Option for display of application passwords in AccessAssistant.		Password display option in AccessAssistant	#0: Disable viewing of passwords #1: Display password, no option to copy to clipboard *#2: Display password by default, with option to copy to clipboard #3: Copy to clipboard by default, with option to display password (refreshed on sync)	System

AccessAudit policies

pid_audit_custom_events_list				
List of custom audit event codes and their corresponding display names. <i>Note: AccessProfiles should be written to detect the events and submit appropriate custom audit logs.</i>		List of custom audit events	Each custom event is represented by one string of the form: event_code,display_name event_code should be a hexadecimal value in the range: 0x43015000 to 0x43015FFF (multiple allowed) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

AccessAgent policies

EnGINA policies

pid_engina_winlogon_option_enabled

Whether to enable the option to go to Windows logon directly from EnGINA.	[DO] "EnginaWinlogonOptionEnabled"	Allow logon bypass through Windows?	*#True #False *#1: Yes #0: No (refreshed on use)	Machine
---	---------------------------------------	-------------------------------------	--	---------

pid_engina_app_launch_enabled

Whether to enable the launching of an application from EnGINA welcome or locked screen.	[DO] "EnginaAppLaunchEnabled"	Enable application launch from EnGINA?	#True *#False *#0: No #1: Yes (refreshed on use)	Machine
---	----------------------------------	--	--	---------

pid_engina_app_launch_label

Display label for the link on EnGINA welcome or locked screen, for launching an application. <i>Note: Effective only if pid_engina_app_launch_enabled is 1.</i>	[DO] "EnginaAppLaunchLabel"	Display label for application launch	(refreshed on use)	Machine
--	--------------------------------	--------------------------------------	--------------------	---------

pid_engina_app_launch_cmd

Command line for launching an application from EnGINA welcome or locked screen. Notes: 1. <i>Effective only if pid_engina_app_launch_enabled is 1.</i> 2. <i>If the application is launched from welcome screen, the owner of the process for the application will be "System".</i> 3. <i>If the application is launched from locked screen, the owner of the process for the application will be "currently logged on desktop user".</i>	[DO] "EnginaAppLaunchCmd"	Command line for application launch	(refreshed on use)	Machine
--	------------------------------	-------------------------------------	--------------------	---------

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------


pid_engina_bypass_hot_key_enabled				
<p>Whether EnGINA Bypass Hot Key is enabled.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If enabled, user can press the EnGINA Bypass Hot Key sequence to bypass EnGINA and go to Windows to log on or unlock. 2. Hot Key is accepted at any of the following EnGINA states: Welcome, Log On, Computer Locked, Unlock This Computer. 3. If Hot Key is pressed at computer locked screen, AccessAgent will not ask the user for confirmation on whether to log off previous user, even though there can be a previous user logged on to the computer. Microsoft GINA will be presented to user, but it will allow unlocking only by the same user or Administrator. 	<p>[DO]</p> <p>"EnginaBypass-HotKeyEnabled"</p>	<p>Enable EnGINA Bypass Hot Key?</p>	<p>*#1: Yes</p> <p>#0: No</p> <p>*#True</p> <p>#False</p> <p>(refreshed on start-up)</p>	<p>Machine System</p>

pid_engina_bypass_hot_key_sequence				
<p>The EnGINA Bypass Hot Key sequence.</p> <p>Note:</p> <p>Effective only if <code>pid_engina_bypass_hot_key_enabled</code> is enabled.</p>	<p>[DO]</p> <p>"EnginaBypass-HotKeySequence"</p>	<p>EnGINA Bypass Hot Key sequence</p>	<p>*#Ctrl</p> <p>*#Alt</p> <p>*#Home</p> <p>(max 3 keys from set of: Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E}, except for Ctrl-Alt-Del, which is not allowed)</p> <p>(2 of the keys in this set should be used so that the probability of conflict with other applications is minimized: Ctrl, Shift, Alt)</p> <p>(refreshed on start-up)</p>	<p>Machine System</p>

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

pid_engina_bypass_automatic_enabled				
<p>Whether automatic EnGINA Bypass is enabled.</p> <p>Notes:</p> <p>1. If enabled, IMS Server is not contactable, and user's Wallet is not cached, AccessAgent will automatically bypass EnGINA and show Microsoft GINA when user attempts to log on or unlock. A configurable text message is shown (<i>pid_engina_bypass_automatic_text</i>) in a prompt with an OK button.</p> <p>2. If <i>pid_unlock_option</i> is 4, AccessAgent will first prompt whether to log off previous user. If user clicks Yes, <i>pid_enc_pwd_is_ad_pwd_enabled</i> is True, IMS Server is not contactable, and user's Wallet is not cached, AccessAgent will prompt user with configurable text message (<i>pid_engina_bypass_automatic_text</i>). After user clicks OK, AccessAgent will log off the previous user's desktop and automatically bring the new user to the Microsoft GINA's logon screen.</p> <p>3. This feature does not support logon with 2nd factors.</p>	<p>[DO] "EnginaBypassAutomaticEnabled"</p>	<p>Enable automatic EnGINA bypass?</p>	<p>#True *#False</p> <p>#1: Yes *#0: No (refreshed on startup)</p>	<p>Machine</p>

pid_engina_bypass_automatic_text				
<p>Configurable text message for automatic EnGINA bypass</p>		<p>Message for automatic EnGINA bypass</p>	<p>*AccessAgent is currently unable to connect to the IMS Server to log on to your Wallet. You may proceed to log on to Windows but automatic sign-on will be disabled. (refreshed on sync)</p>	<p>System</p>

Desktop inactivity policies				
 pid_desktop_inactivity_mins				
<p>Desktop inactivity duration, in minutes, after which AccessAgent may perform a set of actions.</p>	<p>[DO] "DesktopInactivityMins"</p>	<p>Desktop inactivity duration, in minutes</p>	<p>*30 (refreshed on sync for system policy) (refreshed on use for machine policy)</p>	<p>Machine System</p>

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

* pid_desktop_inactivity_action				
<p>Actions to be performed by AccessAgent after a period of desktop inactivity.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This policy is ineffective if computer is already locked. In that case, locked inactivity action would be effective. 2. If user is not logged on to Wallet, the "log off Wallet" actions for policy values 2 and 5 will not be performed. 	<p>[DO]</p> <p>"DesktopInactivityAction"</p>	<p>Desktop inactivity actions</p>	<p>*#0: No action</p> <p>#1: Log off Windows</p> <p>#2: Log off Wallet</p> <p>#4: Lock computer</p> <p>#5: Log off Wallet and lock computer (refreshed on sync for system policy)</p> <p>(refreshed on use for machine policy)</p>	<p>Machine System</p>

pid_desktop_inactivity_action_countdown_secs				
<p>Confirmation countdown duration, in seconds, for desktop inactivity.</p>	<p>[DO]</p> <p>"DesktopInactivityActionCountdownSecs"</p>	<p>Confirmation countdown duration, in seconds, for desktop inactivity</p>	<p>*5</p> <p>(0 to disable confirmation countdown)</p> <p>(refreshed on sync for system policy)</p> <p>(refreshed on use for machine policy)</p>	<p>Machine System</p>

pid_win_screensaver_action				
<p>Actions to be performed by AccessAgent on Windows screen saver activation.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If this policy triggers a computer lock, desktop inactivity action becomes ineffective. 2. If this policy triggers a screen saver without password protection, desktop inactivity action would still remain effective while screen saver is on. 3. This policy allows a 2-level desktop inactivity behavior. If this policy is set to 1, desktop inactivity mins is set to 4, and the Windows screen saver is set to time-out in 2 minutes and not password protected, then the computer will show screen saver after 2 minutes of idling and be locked after an additional 2 minutes of idling. 	<p>[DO]</p> <p>"WinScreensaverAction"</p>	<p>Actions on Windows screen saver activation</p>	<p>#0: Disable Windows screen saver</p> <p>#1: If screen saver is password protected, lock computer, else show normal screen saver</p> <p>*#2: Lock computer (refreshed on sync for system policy)</p> <p>(refreshed on use for machine policy)</p>	<p>Machine System</p>

pid_locked_computer_inactivity_mins				
<p>Locked computer inactivity duration, in minutes, after which AccessAgent may perform a set of actions.</p>	<p>[DO]</p> <p>"LockedComputerInactivityMins"</p>	<p>Locked computer inactivity duration, in minutes</p>	<p>*30</p> <p>(refreshed on sync for system policy)</p> <p>(refreshed on use for machine policy)</p>	<p>Machine System</p>

Description	Registry	IMS Entry	Values	Scope
pid_locked_computer_inactivity_action				
<p>Actions to be performed by AccessAgent after a period of desktop inactivity while computer is locked and user is logged on to Wallet.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <code>pid_lusm_sessions_max = 1</code>. 2. This policy is effective only if EnGINA screen lock is shown. 	<p>[DO] "LockedComputerInactivityAction"</p>	<p>Locked computer inactivity actions when user is logged on to Wallet</p>	<p>*#0: No action #1: Log off Windows (refreshed on sync for system policy) (refreshed on use for machine policy)</p>	<p>Machine System</p>

Lock policies

pid_lock_option

<p>Type of screen lock to be used when computer is locked.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If <code>pid_lusm_sessions_max > 1</code>, only policy 1 (EnGINA screen lock) is supported. 2. From transparent screen lock, user can trigger an unlock or switch user by presenting a 2nd factor. 3. From transparent screen lock, AccessAgent UI is displayed when Encentuate Hot Key is pressed. From this screen, user can manually log off AccessAgent, which will unlock the computer, and actions specified by <code>pid_logoff_manual_action</code> will be performed. <p>The "log off" action will be available regardless of the setting for <code>pid_logoff_manual_while_locked_option_enabled</code>.</p> <ol style="list-style-type: none"> 4. Even after transparent screen lock is activated, the action specified by <code>pid_desktop_inactivity_action</code> will still be carried out after a period of desktop inactivity has elapsed. Hence, <code>pid_desktop_inactivity_action</code> is recommended to be set to 4. 	<p>[DO] "LockOption"</p>	<p>Screen lock option</p>	<p>#1: EnGINA screen lock #2: Transparent screen lock (refreshed on use) PublicAdmin</p>	<p>Machine</p>
---	------------------------------	---------------------------	--	----------------

pid_lock_transparent_text

<p>Configurable text for transparent screen lock.</p> <p>Note: Effective only if <code>pid_lock_option</code> is 2.</p>	<p>[DO] "LockTransparentText"</p>	<p>Transparent screen lock message</p>	<p>*Tap your RFID card or Ctrl-Alt-E to unlock. (text box takes about 40 chars) (refreshed on use)</p>	<p>Machine</p>
---	---------------------------------------	--	--	----------------

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

pid_lock_transparent_hot_key_enabled				
<p>Whether the "Ctrl-Esc" Hot Key sequence is enabled during transparent screen lock.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <i>pid_lock_option</i> is 2 and transparent screen lock is shown. 2. If enabled, this Hot Key is equivalent to the <i>Encentuate</i> Hot Key when computer is locked. When pressed, <i>AccessAgent</i> UI is shown on the transparent screen lock. 3. This additional Hot Key is useful for remote access systems (e.g., <i>LANDesk</i>) that can send only limited key sequences. 	<p>[DO]</p> <p>"LockTransparentHotKeyEnabled"</p>	<p>Enable transparent screen lock hot key?</p>	<p>#True</p> <p>*#False</p> <p>*#0: No</p> <p>#1: Yes</p> <p>(refreshed on use)</p>	Machine

Lock/Unlock policies				
pid_unlock_with_win_option				
<p>Option for unlocking using Windows unlock.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Policy should be set to 1 for personal workstations, if desired, and 2 for shared workstations. 2. Policy should be set to 0 if <i>pid_lusm_sessions_max</i> > 1. 3. <i>AccessAgent</i> is logged off when computer is unlocked using Windows unlock. 	<p>[DO]</p> <p>"UnlockWithWinOption"</p>	<p>Option for allowing unlock bypass through Windows</p>	<p>#0: Disabled</p> <p>*#1: Windows unlock is always available</p> <p>#2: Windows unlock is available only if <i>AccessAgent</i> is not logged on</p> <p>(refreshed on use)</p>	Machine

pid_unlock_different_user_action_countdown_secs				
<p>Confirmation countdown duration, in seconds, for unlocking by a different user.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <i>pid_lusm_sessions_max</i> = 1. 2. Effective when a user attempts to unlock computer while another user has already been logged on to <i>AccessAgent</i>. 3. If policy value is non-zero, user can click on the prompt to cancel switch user. If user does not confirm, <i>AccessAgent</i> will proceed to unlock the computer. 	<p>[DO]</p> <p>"UnlockDifferentUserActionCountdownSecs"</p>	<p>Confirmation countdown duration, in seconds, for unlocking by a different user</p>	<p>*0</p> <p>(0 to disable confirmation countdown)</p> <p>(refreshed on sync for user policy)</p> <p>(refreshed on use for machine policy)</p>	Machine User

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

* pid_unlock_option				
<p>Unlock computer policy for controlling who is allowed to unlock a computer when it has been locked by a user who is logged on to AccessAgent.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <i>pid_lusm_sessions_max</i> = 1. 2. Same user refers to the same Encen- tuate user who locked the computer (i.e., same user name). 3. Admin refers to Windows user with Administrator privilege on that com- puter, i.e., the Wallet should contain Windows credentials of an Admin user on that computer. 4. This policy is ignored if <i>pid_lock_option</i> = 2 (transparent screen lock). In transparent screen lock mode, any user is always allowed to unlock the computer. 5. For policy 3, if a different user tries to unlock, AA unlocks computer and brings the user to the current desktop, but it logs on to new Wallet after log- ging off the old one. 6. For policy 4, only the same user can unlock computer and bring the user to the current desktop. For any other users, AA logs off from old desktop and logs on to new Wallet. AA shall not require user to present 2nd factor one more time. If new Wallet does not have a desktop account on the computer, user would need to log on to Windows too. This option is currently not sup- ported for ARFID. 	[DO] "UnlockOption"	Unlock com- puter policy	<p>#1: Only the same user can unlock</p> <p>*#3: Any user with or without current desktop account in Wallet can unlock</p> <p>#4: Only the same user can unlock, but different user can re- log on to Windows (refreshed on sync for user policy)</p> <p>(refreshed on use for machine policy)</p>	Machine User
pid_script_unlock_type				
<p>Type of unlock script to be run.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <i>pid_script_unlock_enabled</i> is enabled. 2. See <i>pid_script_unlock_enabled</i>. 		Unlock script type	<p>*#1: Batch</p> <p>#2: VBScript (refreshed on sync)</p>	User

Description	Registry	IMS Entry	Values	Scope
pid_script_unlock_enabled				
<p>Whether to enable running of unlock script when user unlocks an existing AccessAgent session.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. The unlock script is only executed if user already has an existing AccessAgent session and is unlocking it. 2. The unlock script is not executed if user is unlocking a shared workstation that is logged on with a generic Windows account, and not currently logged on to AccessAgent. In this case, the logon script (see <code>pid_script_logon_enabled</code>) will be executed instead. 3. The unlock script can be used in Local User Session Management (LUSM) to auto-launch single-instance applications that may have been terminated by other users who are logged on to the same workstation. 4. Unlock script is not supported if <code>pid_lock_option</code> is 2 (such as transparent screen lock is used). 		<p>Enable unlock script when user unlocks an existing AccessAgent session?</p>	<p>#True *#False (refreshed on sync)</p>	User
pid_script_unlock_code				
<p>Source code of unlock script to be run.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <code>pid_script_unlock_enabled</code> is enabled. 2. See <code>pid_script_unlock_enabled</code>. 		<p>Unlock script code</p>	<p>(refreshed on sync)</p>	User
pid_script_lock_type				
<p>Type of lock script to be run.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <code>pid_script_lock_enabled</code> is enabled. 2. See <code>pid_script_lock_enabled</code>. 		<p>Lock script type</p>	<p>*#1: Batch #2: VBScript (refreshed on sync)</p>	User
pid_script_lock_code				
<p>Source code of lock script to be run.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <code>pid_script_lock_enabled</code> is enabled. 2. See <code>pid_script_lock_enabled</code>. 		<p>Lock script code</p>	<p>(refreshed on sync)</p>	User

Description	Registry	IMS Entry	Values	Scope
pid_script_lock_enabled				
<p>Whether to enable running of lock script during locking of the user's AccessAgent session.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. The lock script is only executed if user's session is currently visible during locking. That is, in Local User Session Management (LUSM), currently invisible user sessions will not have lock script executed. 2. The lock script is executed regardless of whether the locking is due to desktop inactivity or manually triggered (e.g., pressing Win-L or tapping RFID card). 3. The lock script is useful for closing applications when a "guest" AccessAgent session is being locked. It can also be used in conjunction with the unlock script in a Local User Session Management (LUSM) scenario to record any single-instance applications that may be running before locking, which may have to be relaunched during unlock. 		<p>Enable lock script during locking of the user's AccessAgent session?</p>	<p>#True *#False (refreshed on sync)</p>	User

USB Key policies

pid_usb_key_removal_action				
<p>Actions to be performed when USB Key is removed.</p> <p>Note:</p> <p>Currently, this is supported only if <code>pid_lusm_sessions_max = 1</code>. In future, if <code>pid_lusm_sessions_max > 1</code>, AA with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen.</p>	<p>[DO] "UsbKeyRemovalAction"</p>	<p>USB Key removal actions</p>	<p>#1: Log off Windows #2: Log off Wallet *#4: Lock computer #5: Log off Wallet and lock computer (refreshed on sync for user policy) (refreshed on use for machine policy)</p>	<p>Machine User</p>

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

RFID policies				
* pid_rfid_tap_same_action				
<p>Actions to be performed by AccessAgent when the currently logged on user taps the RFID card on desktop.</p> <p>Notes:</p> <p>1. This policy is not applicable if the user did not log on using RFID.</p> <p>2. If pid_lusm_sessions_max > 1, AA with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen.</p>	<p>[DO]</p> <p>"RfidTapSameAction"</p>	<p>Actions on tapping same RFID on desktop</p>	<p>*#0: No action</p> <p>#1: Log off Windows</p> <p>#2: Log off Wallet</p> <p>#4: Lock computer</p> <p>#5: Log off Wallet and lock computer (refreshed on sync for user policy)</p> <p>(refreshed on use for machine policy)</p>	<p>Machine User</p>
pid_rfid_tap_same_action_countdown_secs				
<p>Confirmation countdown duration, in seconds, for tapping same RFID on desktop.</p>	<p>[DO]</p> <p>"RfidTapSameActionCountdownSecs"</p>	<p>Confirmation countdown duration, in seconds, for tapping same RFID on desktop</p>	<p>*5</p> <p>(0 to disable confirmation countdown: not recommended to prevent accidental double detection of RFID tap)</p> <p>(refreshed on sync for user policy)</p> <p>(refreshed on use for machine policy)</p>	<p>Machine User</p>
* pid_rfid_only_unlock_enabled				
<p>Whether to allow RFID-only unlock (without password) by the same user who locked the computer, if unlock happens within the duration specified by pid_rfid_only_unlock_timeout_secs.</p> <p>Note:</p> <p>Also applies to Active Proximity Badge. But if pid_lusm_sessions_max > 1, the Active Proximity Badge only unlock is applicable only for the last visible user desktop.</p>	<p>[DO]</p> <p>"RfidOnlyUnlockEnabled"</p>	<p>Enable RFID-only unlock?</p>	<p>#1: Yes</p> <p>*#0: No</p> <p>#True</p> <p>*#False</p> <p>(refreshed on sync for user policy)</p> <p>(refreshed on use for machine policy)</p>	<p>Machine User</p>

Description	Registry	IMS Entry	Values	Scope
* pid_rfid_only_unlock_timeout_secs				
<p>Time expiry, in seconds, for RFID-only unlock. After this duration (timed from last lock), RFID only unlock will not be allowed.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <i>pid_rfid_only_unlock_enabled</i> is enabled. 2. Also applies to Active Proximity Badge. 	<p>[DO] "RfidOnlyUnlock-TimeoutSecs"</p>	<p>Time expiry, in seconds, for RFID-only unlock</p>	<p>*0 (0 to disable expiry, such as always allow RFID-only unlock) (refreshed on sync for user policy) (refreshed on use for machine policy)</p>	<p>Machine User</p>
* pid_rfid_only_logon_enabled				
<p>Whether to allow RFID-only logon (without password) by a user who has recently logged on using RFID and password on the same or another computer, if logon happens within the duration specified by <i>pid_rfid_only_logon_timeout_mins</i>.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. RFID-only logon will only work if IMS Server is online and user has an existing cached Wallet on the computer. 2. RFID-only logon is tied to the specific RFID card used for logon. If user has two RFID cards and card #1 was used to log on, user can use RFID-only logon only with card #1. If attempting to log on with card #2, user should be prompted for password. 3. For better security, <i>pid_wallet_cache_max_inactivity_days</i> should be used to clear inactive Wallets, so that exposure of RFID-only logon is only limited to those computers that a particular user frequently uses. 4. RFID-only logon is not supported if <i>pid_lusm_sessions_max</i> > 1. 	<p>[DO] "RfidOnlyLogonEnabled"</p>	<p>Enable RFID-only logon?</p>	<p>#True *#False #1: Yes *#0: No (refreshed on use)</p>	<p>Machine</p>
* pid_rfid_only_logon_timeout_mins				
<p>Time expiry, in minutes, for RFID-only logon. After this duration (timed from last logon with RFID and password), RFID-only logon will not be allowed.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <i>pid_rfid_only_logon_enabled</i> is enabled. 2. Time-out is refreshed upon every logon to AccessAgent with RFID and password. 		<p>Time expiry, in minutes, for RFID-only logon</p>	<p>*480 (0 to disable RFID-only logon) (refreshed on sync)</p>	<p>User</p>

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

* pid_rfid_tap_different_action				
<p>Actions to be performed by AccessAgent when an RFID card that does not belong to the currently logged on user is tapped on desktop.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If <code>pid_rfid_display_utility_enabled</code> is 1, this policy is not effective. 2. This policy is applicable even if the current user did not use RFID to log on. 3. For policy value 8, AA shall not require new user to tap RFID again after logging off from Windows. 4. If <code>pid_lusm_sessions_max</code> > 1, AA with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen. AA with policy value 6 (Switch user) will attempt to create a user desktop session for the new user. AA with policy value 8 (Log off Windows and log on as new user) will log off the current user's desktop session and create a user desktop session for the new user. 	<p>[DO]</p> <p>"RfidTapDifferentAction"</p>	<p>Actions on tapping different RFID on desktop</p>	<p>*#0: No action</p> <p>#4: Lock computer</p> <p>#5: Log off Wallet and lock computer</p> <p>#6: Switch user</p> <p>#8: Log off Windows and log on as new user</p> <p>(refreshed on sync for user policy)</p> <p>(refreshed on use for machine policy)</p>	<p>Machine</p> <p>User</p>

pid_rfid_tap_different_action_countdown_secs				
<p>Confirmation countdown duration, in seconds, for tapping different RFID on desktop.</p>	<p>[DO]</p> <p>"RfidTapDifferentActionCountdownSecs"</p>	<p>Confirmation countdown duration, in seconds, for tapping different RFID on desktop</p>	<p>*5</p> <p>(0 to disable confirmation countdown: recommended only when RFID tap different action is 6, to prevent accidental double detection of RFID tap)</p> <p>(refreshed on sync for user policy)</p> <p>(refreshed on use for machine policy)</p>	<p>Machine</p> <p>User</p>

pid_rfid_display_utility_enabled				
<p>Whether to display the registration status of an RFID card that does not belong to the currently logged on user when it is tapped on desktop.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If policy value is 1, this policy overrides <code>pid_rfid_tap_different_action</code>. If RFID card is registered, the user name is displayed in a prompt. 2. This display utility will only work when AccessAgent is logged on. 	<p>[DO]</p> <p>"RfidDisplayUtilityEnabled"</p>	<p>Enable RFID display utility?</p>	<p>#True</p> <p>*#False</p> <p>*#0: No</p> <p>#1: Yes</p> <p>(refreshed on use)</p>	<p>Machine</p>

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

Active Proximity Badge policies				
pid_arfid_presentation_range_max				
Maximum range for recognizing that an active proximity badge is presented.	[DO] "ArfidPresentationRangeMax"	Maximum range for recognizing that an active proximity badge is presented	*3 (from 1 to 16) (should be Active Proximity Badge removal range minimum - 3) (3 for near, 5 for medium, 7 for far) (refreshed on use)	Machine System

pid_arfid_removal_range_min				
Minimum range for recognizing that an active proximity badge is removed.	[DO] "ArfidRemovalRangeMin"	Minimum range for recognizing that an active proximity badge is removed	*7 (from 4 to 19) (should be Active Proximity Badge presentation range max + 3) (7 for near, 9 for medium, 13 for far) (refreshed on use)	Machine System

Fingerprint policies				
* pid_fingerprint_tap_same_action				
<p>Actions to be performed by AccessAgent when the currently logged on user taps finger on the reader.</p> <p>Note:</p> <p>1. This policy is not applicable if the user did not log on using fingerprint.</p> <p>2. Currently, this is supported only if pid_lusm_sessions_max = 1. In future, if pid_lusm_sessions_max > 1, AA with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen.]</p>	[DO] "FingerprintTapSameAction"	Actions on tapping same finger on desktop	*#0: No action #1: Log off Windows #2: Log off Wallet #4: Lock computer #5: Log off Wallet and lock computer (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User

Description	Registry	IMS Entry	Values	Scope
pid_fingerprint_tap_same_action_countdown_secs				
Confirmation countdown duration, in seconds, for tapping same finger on desktop.	[DO] "FingerprintTap-SameAction-CountdownSecs"	Confirmation countdown duration, in seconds, for tapping same finger on desktop	*5 (0 to disable confirmation countdown: not recommended to prevent accidental double detection of finger tap) (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User
pid_fingerprint_tap_different_action_countdown_secs				
Confirmation countdown duration, in seconds, for tapping different finger on desktop.	[DO] "FingerprintTap-DifferentAction-CountdownSecs"	Confirmation countdown duration, in seconds, for tapping different finger on desktop	*5 (0 to disable confirmation countdown: recommended only when fingerprint tap different action is 6, to prevent accidental double detection of finger tap) (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User
pid_fingerprint_registration_max				
Maximum number of fingerprints that each user should be allowed to register. <i>Note: If the value of this policy is reduced, a user who has already registered more fingerprints than allowed by the new policy value will still be allowed to log on with any of the fingerprints that have been registered. However, if attempting to register a new fingerprint, an existing fingerprint will have to be replaced. The user will not be able to increase the number of fingerprints registered.</i>		Maximum number of fingerprints that can be registered per user	(from 1 to 10) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
* pid_fingerprint_tap_different_action				
<p>Actions to be performed by AccessAgent when a finger that does not belong to the currently logged on user is tapped on desktop.</p> <p>Notes:</p> <p>1. This policy is applicable even if the current user did not use fingerprint to log on.</p> <p>2. For policy value 8, AA shall not require new user to tap RFID again after logging off from Windows.</p> <p>3. Currently, this is supported only if pid_lusm_sessions_max = 1. In future, if pid_lusm_sessions_max > 1, AccessAgent with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen. AccessAgent with policy value 6 (Switch user) will attempt to create a user desktop session for the new user. AccessAgent with policy value 8 (Log off Windows and log on as new user) will log off the current user's desktop session and create a user desktop session for the new user.</p>	<p>[DO]</p> <p>"FingerprintTap-DifferentAction"</p>	<p>Actions on tapping different finger on desktop</p>	<p>*#0: No action</p> <p>#4: Lock computer</p> <p>#5: Log off Wallet and lock computer</p> <p>#6: Switch user</p> <p>#8: Log off Windows and log on as new user</p> <p>(refreshed on sync for user policy)</p> <p>(refreshed on use for machine policy)</p>	<p>Machine</p> <p>User</p>

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

Terminal Server/Roaming session policies				
pid_machine_type_ts				
<p>Whether the machine is a Terminal Server or Citrix server.</p> <p>Notes:</p> <p><i>This policy should be set to 1 on the remote AccessAgent (i.e., on the Terminal Server or Citrix server).</i></p> <p><i>If this policy is 1, AccessAgent behaves as a remote AccessAgent:</i></p> <ol style="list-style-type: none"> 1. It synchronizes itself with the local AA (only for Terminal Server). 2. pid_second_factors_supported_list is not effective. It is treated as an empty list. 3. "Lock computer" options from the WNA and AccessAgent UI are disabled, if logon to remote AccessAgent is performed using credentials submitted by local AccessAgent (only for Terminal Server). 4. Uses pid_ts_second_factor_bypass_option to determine its behavior when user's authentication policy requires 2nd factor for logon. <p><i>The following combinations of policy settings are not supported (behavior is unpredictable):</i></p> <ul style="list-style-type: none"> - policy value 0 on a Terminal Server or Citrix server installation - policy value 1 on a client machine installation. 	<p>[DO]</p> <p>"MachineTypeTS"</p>		<p>#1: Machine is Terminal Server</p> <p>*#0: Machine is not Terminal Server (refreshed on startup)</p>	Machine

pid_ts_logon_prompt_enabled				
<p>Whether to launch AccessAgent logon dialog if AccessAgent is not logged on while a Terminal Server session or Citrix application is launched.</p> <p>Note: <i>This policy should be set on the remote AccessAgent (such as on the Terminal Server or Citrix server).</i></p>	<p>[DO]</p> <p>"TSLogon-PromptEnabled"</p>	<p>Enable auto-launching of AccessAgent logon prompt?</p>	<p>#True</p> <p>*#False</p> <p>*#0: No</p> <p>#1: Yes (refreshed on use)</p>	Machine

Description	Registry	IMS Entry	Values	Scope
pid_ts_logon_cache_enabled				
<p>Whether to cache the Wallet logon credentials on the Terminal Server or Citrix server so that AA can automatically log on to Wallet.</p> <p><i>Note: This policy should be set on the remote AccessAgent (such as on the Terminal Server or Citrix server).</i></p>	[DO] "TSLogon-CacheEnabled"	Enable caching of Wallet logon credentials?	#True *#False *#0: No #1: Yes (refreshed on use)	Machine
pid_ts_lock_local_computer_action				
<p>Option to disconnect the Terminal Server session, and/or log off the remote AccessAgent while locking the local computer.</p> <p><i>Notes: Only supported on Terminal Server but not Citrix server.</i></p>		Actions on remote session while locking local computer	#0: No action #1: Disconnect remote session #2: Log off remote AccessAgent and disconnect remote session #3: Log off remote session #4: Log off remote AccessAgent (refreshed on sync)	User
pid_ts_logoff_local_session_action				
<p>Option to disconnect the Terminal Server session, and/or log off the remote AccessAgent before logging off the local AccessAgent.</p> <p><i>Notes: Only supported on Terminal Server but not Citrix server.</i></p>		Actions on remote session before logging off local session	*#0: No action #1: Disconnect remote session #2: Log off remote AccessAgent and disconnect remote session #3: Log off remote session #4: Log off remote AccessAgent (refreshed on sync)	User
pid_ts_engina_logon_no_local_session_enabled				
<p>Whether to use EnGINA logon or Microsoft GINA logon for the Terminal Server session, when there is no local AccessAgent session.</p> <p><i>Notes:</i></p> <p>1. This policy should be set on the remote AccessAgent (such as on the Terminal Server or Citrix server).</p> <p>2. This policy should be set to 0 on Citrix servers.</p>	[DO] "TSEnginaLogon-NoLocalSession-Enabled"	Use EnGINA logon when there is no local AccessAgent session?	#True *#False *#0: No #1: Yes (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_ts_logoff_on_reconnect_no_local_session_enabled				
<p>Whether to log off remote AccessAgent when user, with no local AccessAgent session, reconnects to an existing session on Terminal Server.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Only supported on Terminal Server but not Citrix server. 2. This policy should be set on the remote AccessAgent (i.e., on the Terminal Server). 3. This policy is effective only if there is no local AccessAgent session on the user's client machine. 4. This policy should be set to 1 if users use a generic Windows account to log on to remote session. Logging off the remote AccessAgent ensures that the next user is not able to use the previous user's Wallet and applications. 5. The usual logoff actions (auto-logoff of applications and running of logoff script) are performed when remote AccessAgent is logged off. 6. If pid_ts_logon_prompt_enabled is set to 1, remote AccessAgent prompts user to log on after the previous user has been logged off. 	<p>[DO]</p> <p>"TSLogoffOnReconnectNoLocalSessionEnabled"</p>	<p>Log off remote AccessAgent when reconnecting from workstation without local AccessAgent session?</p>	<p>#True</p> <p>*#False</p> <p>*#0: No</p> <p>#1: Yes (refreshed on use)</p>	Machine
pid_ts_delay_app_launch_exe_list				
<p>The list of applications which should be delayed from launching until remote AccessAgent is ready to perform automatic sign-on.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This policy should be set on the remote AccessAgent (such as on the Citrix server). 2. Effective only if pid_ts_delay_app_launch_enabled is enabled. 3. Each application should be indicated by its executable name (e.g., "notepad.exe"). 	<p>[DO]</p> <p>"TSDelayAppLaunchExeList"</p>	<p>Applications to be delayed from launching on Citrix server</p>	<p>(refreshed on use)</p>	Machine

Description	Registry	IMS Entry	Values	Scope
pid_ts_delay_app_launch_enabled				
<p>Whether to enable the delaying of application launch for Citrix server.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Currently, this feature is only applicable to Citrix. It is not applicable to Terminal Server access using RDP. 2. This policy should be set on the remote AccessAgent (i.e., on the Citrix server). 3. If this feature is not enabled for an application, user may see the application's logon prompt first before remote AccessAgent is ready to perform automatic sign-on, and hence, causing some confusion to the user. Enabling this feature for an application will ensure that remote AccessAgent is ready to perform automatic sign-on when user sees the logon prompt. 	<p>[DO] "TSDelayAppLaunchEnabled"</p>	<p>Delay application launch for Citrix server?</p>	<p>#True *#False</p> <p>#1: Yes *#0: No (refreshed on use)</p>	Machine
pid_ts_start_aa_no_local_aa_enabled				
<p>Whether to start remote AccessAgent while a Terminal Server session is launched if local AccessAgent is not present.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Only supported on Terminal Server but not Citrix server. 2. This policy should be set on the remote AccessAgent (such as on the Terminal Server). 3. This policy only applies to launching of published applications. If a remote desktop is launched, remote AccessAgent will always be started. 4. For policy value 0, users will not be able to log on to remote AccessAgent from machines that do not have local AccessAgent installed (e.g., home or Internet café). 	<p>[DO] "TSSStartAANoLocalAAEnabled"</p>	<p>Launch remote AccessAgent even if local AccessAgent is not present?</p>	<p>*#True #False</p> <p>#0: No *#1: Yes (refreshed on use)</p>	Machine

Description	Registry	IMS Entry	Values	Scope
pid_ts_delay_app_launch_timeout_secs				
<p>Time-out, in secs, for delaying of application launch.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This policy should be set on the remote AccessAgent (such as on the Citrix server). 2. Effective only if <code>pid_ts_delay_app_launch_enabled</code> is enabled. 3. Remote AccessAgent will, first, wait for connection to be established with local AccessAgent. If connection is not established within the time-out duration, application proceeds to launch. 4. If local AccessAgent manages to establish connection with remote AccessAgent, remote AccessAgent will wait for another time-out period for automatic sign-on to be ready. If remote AccessAgent is not ready for automatic sign-on within the time-out duration, application proceeds to launch. 5. Hence, user may potentially have to wait up to two times the time-out duration if local AccessAgent manages to establish connection with remote AccessAgent just before the first time-out duration lapses. 	<p>[DO]</p> <p>"TSDelayAppLaunchTimeoutSecs"</p>	<p>Time-out, in seconds, for delaying of application launch</p>	<p>*10</p> <p>(refreshed on use)</p>	<p>Machine</p>
pid_com_redir_enabled				
<p>Whether the device monitoring mechanism should perform COM port redirection from the client machine (connecting to the Terminal Server) to the Terminal Server.</p> <p>Note:</p> <p>If enabled for AA on Terminal Server or Citrix server, authentication devices on remote client machines (e.g., for thin clients where there is no AA installed) can be monitored. AA would map a virtual COM port (<code>pid_com_redir_local_virtual_port</code>) on the Terminal Server or Citrix server to a physical COM port (<code>pid_com_redir_remote_physical_port</code>) on the remote client.</p>	<p>[DO]</p> <p>"ComRedirEnabled"</p>	<p>Enable COM port redirection?</p>	<p>#True</p> <p>*#False</p> <p>*#0: No</p> <p>#1: Yes</p> <p>(refreshed on startup)</p>	<p>Machine</p>

Description	Registry	IMS Entry	Values	Scope
pid_ts_aa_menu_option				
<p>Whether to display menu options on AccessAgent user interface in a Terminal Server session.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Only supported on Terminal Server but not Citrix server. 2. If policy value is 1, only "Remote session information" is displayed when there is local AccessAgent session. Full menu options are displayed when there is no local AccessAgent session. Same applies to right-click menu options for AccessAgent icon at Windows notification area. 3. If policy value is 2, all menu options are displayed except for "Lock this computer" when there is local AccessAgent session. Full menu options are displayed when there is no local AccessAgent session. Same applies to right-click menu options for AccessAgent icon at Windows notification area. This option is recommended for Roaming Desktop configuration. 	<p>[DO] "TSAaMenuOption"</p>	<p>Option for displaying menu options on remote AccessAgent</p>	<p>*#1: Display menu options only if there is no local AccessAgent session #2: Always display all menu o</p>	Machine
pid_com_redir_local_virtual_port				
<p>Virtual COM port on the Terminal Server to which data from the client COM port will get redirected to.</p> <p>Note:</p> <p>Effective only if <code>pid_com_redir_enabled</code> is 1.</p>	<p>[DO] "ComRedirLocalVirtualPort"</p>	<p>Virtual COM port on Terminal Server</p>	<p>*1 (refreshed on startup) (from 1 to 8)</p>	Machine
pid_com_redir_remote_physical_port				
<p>Physical COM port on the client to which the authentication device (e.g., RFID reader) is connected to. The redirection will take place from this port to the Terminal Server's virtual COM port.</p> <p>Note:</p> <p>Effective only if <code>pid_com_redir_enabled</code> is 1.</p>	<p>[DO] "ComRedirRemotePhysicalPort"</p>	<p>Physical COM port on client machine</p>	<p>*1 (refreshed on startup) (min 1)</p>	Machine

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

Logon/Logoff policies				
pid_en_network_provider_enabled				
<p>Whether to enable the Encentuate Network Provider (EnNetworkProvider).</p> <p><i>Notes:</i></p> <p>1. Effective only if EnNetworkProvider has been installed by AccessAgent installer.</p> <p>2. If enabled, AccessAgent will attempt to automatically log on to itself using the credentials provided at Microsoft GINA. It works in conjunction with the AD password synchronization feature so that the same password can be used to log on to Windows as well as AccessAgent.</p>	<p>[DO]</p> <p>"EnNetworkProviderEnabled"</p>	<p>Enable Encentuate Network Provider?</p>	<p>#True</p> <p>*#False</p> <p>#0: No</p> <p>#1: Yes</p> <p>(refreshed on use)</p>	Machine
pid_script_logon_enabled				
<p>Whether to enable running of logon script during user logon.</p>		<p>Enable logon script during user logon?</p>	<p>#True</p> <p>*#False</p> <p>(refreshed on sync)</p>	User
pid_script_logon_type				
<p>Type of logon script to be run.</p> <p><i>Note: Effective only if script logon is enabled.</i></p>		<p>Logon script type</p>	<p>*#1: Batch</p> <p>#2: VBScript</p> <p>(refreshed on sync)</p>	User
pid_script_logon_code				
<p>Source code of logon script to be run.</p> <p><i>Note: Effective only if script logon is enabled.</i></p>		<p>Logon script code</p>	<p>(refreshed on sync)</p>	User

Description	Registry	IMS Entry	Values	Scope
pid_logon_user_name_prefill_option				
<p>Option for pre-filling Encentuate Logon prompt with a user name.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Policy should be set to 0 for shared desktops with many users. 2. Policy should be set to 1 for personal desktops or shared desktops with very few users. 3. Policy should be set to 2 for Terminal Server or Citrix Server. For policy value 2 to work properly, the following Microsoft registry value must be set to 0: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system]dontdisplaylastusername" 	<p>[DO] "LogonUser-NamePrefillOption"</p>	<p>Encentuate user name prefill option</p>	<p>#0: Do not pre-fill</p> <p>*#1: Pre-fill with last logged on user name</p> <p>#2: Pre-fill with currently logged on Windows user name (refreshed on use)</p>	<p>Machine</p>
pid_logon_user_name_display_option				
<p>Option for displaying the name of the currently logged on user.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If this policy is set to 2 or 3, AccessAgent displays the full name of the user, obtained from Active Directory upon logon to Wallet. Hence, the machine will have to be logged on to domain. If AccessAgent fails to obtain the full name from Active Directory, it will fall-back to displaying the Encentuate user name. 2. Due to the limited size of the UI, there is only enough space to display about 20 characters. If the name is truncated, it will be appended with "...". 3. This policy affects all parts of the AccessAgent UI where user name is displayed, for example, main UI, locked screen. 4. In a 2-factor deployment (RFID, USB, etc.), user does not need to enter user name to log on to AccessAgent. But if user forgets 2nd factor, user must enter user name and password to log on to AccessAgent or AccessAssistant. If the full name is always displayed, user may forget the logon user name easily as they do not need to use it every day and also do not see it in the AccessAgent UI. Hence, as a best practice, policy value 1 should be used for a 2-factor deployment. 	<p>[DO] "LogonUserNameDisplayOption"</p>	<p>Encentuate user name display option</p>	<p>*#1: Encentuate user name</p> <p>#2: First name followed by last name</p> <p>#3: Last name followed by first name (refreshed on logon)</p>	<p>Machine</p>

Description	Registry	IMS Entry	Values	Scope
pid_script_logoff_enabled				
Whether to enable running of logoff script during user logoff.		Enable logoff script during user logoff?	#True *#False (refreshed on sync)	User
pid_script_logoff_type				
Type of logoff script to be run. <i>Note: Effective only if script logoff is enabled.</i>		Logoff script type	*#1: Batch #2: VBScript (refreshed on sync)	User
pid_script_logoff_code				
Source code of logoff script to be run. <i>Note: Effective only if script logoff is enabled.</i>		Logoff script code	(refreshed on sync)	User
pid_logoff_manual_enabled				
Whether to allow user to manually log off AccessAgent. <i>Note:</i> <i>If this policy is disabled, the "Log off AccessAgent" option will not appear in any part of AccessAgent UI.</i>	[DO] "LogoffManualEnabled"	Allow user to manually log off AccessAgent?	#0: No *#1: Yes *#True #False (refreshed on sync)	Machine User
* pid_logoff_manual_action				
Actions to be performed by AccessAgent on manual logoff by user. <i>Notes:</i> <i>1. Effective when user manually logs off Wallet from desktop or transparent screen lock.</i> <i>2. If pid_lusm_sessions_max > 1, AccessAgent with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen.</i> <i>This is the recommended policy value for Local User Session Management. If policy value is 2, AccessAgent will be logged off, but user will not be able to re-log on to AccessAgent unless Ctrl-Alt-Del is pressed to log on from the Encountered-replaced Windows security dialog.</i>	[DO] "LogoffManualAction"	Actions on manual logoff by user	#1: Log off Windows *#2: Log off Wallet #4: Log off Wallet and lock computer (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User

Description	Registry	IMS Entry	Values	Scope
pid_logoff_manual_action_countdown_secs				
<p>Confirmation countdown duration, in seconds, for manual logoff by user.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective when user manually logs off Wallet from desktop or locked computer window. 2. If policy value is non-zero, user has to click on the prompt to confirm logoff. If user does not confirm, AccessAgent will not proceed with the logoff. 	<p>[DO]</p> <p>"LogoffManualActionCountdownSecs"</p>	<p>Confirmation countdown duration, in seconds, for manual logoff by user</p>	<p>*30</p> <p>(0 to disable confirmation countdown)</p> <p>(refreshed on sync for user policy)</p> <p>(refreshed on use for machine policy)</p>	<p>Machine User</p>
pid_wallet_logoff_action_for_apps_default				
<p>Default action to take for all applications when user logs off AccessAgent.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If policy value is 1, AccessAgent will attempt to log off all instances of applications. The AccessProfile for each application must contain a logoff action, otherwise the application logoff will not be performed. 2. If policy value is 2, AccessAgent will close all instances of applications that are monitored by AccessAgent. All applications that have AccessProfiles are monitored, regardless of whether AccessAgent is used to log on to the application. 3. This policy is effective whenever a user is logged off from AccessAgent, for example, during a switch user operation. 		<p>Default action for applications, when user logs off AccessAgent</p>	<p>#1: Log off the application</p> <p>#2: Close the application</p> <p>*#3: Do nothing</p> <p>(refreshed on sync)</p>	<p>System</p>
pid_logoff_app_timeout_secs				
<p>Time-out, in secs, for logging off applications.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. When AA logs off a Wallet (during manual logoff or switch user), logging off of applications may occur (depends on configuration). This policy specifies a configurable time-out for logging off applications. 2. If an application is not successfully terminated by its AccessProfile after the time-out, it can be forced to terminate by setting the "Terminate on time-out" and "Time-out" attributes of the "gen_sign_out_trigger" appropriately. 	<p>[DO]</p> <p>"LogoffAppTimeoutSecs"</p>	<p>Time-out, in seconds, for application logoff</p>	<p>*5</p> <p>(from 0 to 60)</p> <p>(refreshed on use)</p>	<p>Machine</p>

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

Encentuate Hot Key policies				
pid_enc_hot_key_enabled				
<p>Whether Encentuate Hot Key is enabled.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. At EnGINA, Hot Key brings user to logon screen. 2. At locked screen, Hot Key brings user to unlock screen. 3. At desktop, if AccessAgent is not logged on, Hot Key launches logon screen. 4. At desktop, if AccessAgent is logged on, Hot Key's behavior is defined by Encentuate Hot Key action. 	<p>[DO]</p> <p>"EncHotKeyEnabled"</p>	<p>Enable Encentuate Hot Key?</p>	<p>*#1: Yes</p> <p>#0: No</p> <p>*#True</p> <p>#False</p> <p>(refreshed on start-up)</p>	<p>Machine System</p>
pid_enc_hot_key_sequence				
<p>The Encentuate Hot Key sequence.</p> <p>Note:</p> <p>Effective only if Encentuate Hot Key is enabled.</p>	<p>[DO]</p> <p>"EncHotKeySequence"</p>	<p>Encentuate Hot Key sequence</p>	<p>*#Ctrl</p> <p>*#Alt</p> <p>*#E</p> <p>(max 3 keys from set of: Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E)</p> <p>(2 of the keys in this set should be used so that the probability of conflict with other applications is minimized: Ctrl, Shift, Alt)</p> <p>(refreshed on start-up)</p>	<p>Machine System</p>
pid_enc_hot_key_action_countdown_secs				
<p>Confirmation countdown duration, in seconds, for pressing Encentuate Hot Key.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if Encentuate Hot Key is enabled. 2. Effective only if Encentuate Hot Key is pressed while AccessAgent is logged on and computer is not locked. 	<p>[DO]</p> <p>"EncHotKeyActionCountdownSecs"</p>	<p>Confirmation countdown duration, in seconds, for pressing Encentuate Hot Key</p>	<p>*5</p> <p>(0 to disable confirmation countdown)</p> <p>(refreshed on sync for system policy)</p> <p>(refreshed on use for machine policy)</p>	<p>Machine System</p>

Description	Registry	IMS Entry	Values	Scope
pid_enc_hot_key_action				
<p>Actions to be performed by AccessAgent if Encentuate Hot Key is pressed at desktop while AccessAgent is logged on.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if Encentuate Hot Key is enabled. 2. Actions taken only if Hot Key is pressed at desktop while AccessAgent is logged on. 3. If <code>pid_lusm_sessions_max > 1</code>, AA with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen. 	<p>[DO]</p> <p>"EncHotKeyAction"</p>	<p>Encentuate Hot Key press actions at desktop when AccessAgent is logged on</p>	<p>#0: No action</p> <p>#1: Log off Windows</p> <p>#2: Log off Wallet</p> <p>#4: Lock computer</p> <p>#5: Log off Wallet and lock computer</p> <p>*#9: Launch AccessAgent window</p> <p>(refreshed on sync for system policy)</p> <p>(refreshed on use for machine policy)</p>	<p>Machine System</p>
pid_enc_hot_key_not_logged_on_action				
<p>Actions to be performed by AccessAgent if Encentuate Hot Key is pressed at desktop while AccessAgent is not logged on.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <code>pid_enc_hot_key_enabled</code> is enabled. 2. Actions taken only if Hot Key is pressed at desktop while AccessAgent is not logged on. 3. If <code>pid_lusm_sessions_max > 1</code>, AccessAgent with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen. <p>However, if the desktop is the default desktop, whether it can be logged off is determined by <code>pid_lusm_default_desktop_preserved_enabled</code>.</p>	<p>[DO]</p> <p>"EncHotKeyNotLoggedOnAction"</p>	<p>Encentuate Hot Key press actions at desktop when AccessAgent is not logged on</p>	<p>#0: No action</p> <p>#1: Log off Windows</p> <p>#4: Lock computer</p> <p>*#9: Launch AccessAgent window</p> <p>(refreshed on sync for system policy)</p> <p>(refreshed on use for machine policy)</p>	<p>Machine System</p>

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

Emergency Hot Key policies				
pid_emergency_hot_key_enabled				
<p>Whether Emergency Hot Key is enabled.</p> <p><i>Notes:</i></p> <ol style="list-style-type: none"> 1. If user presses this Hot Key at computer locked screen, AccessAgent unlocks computer without any credentials but will log off AccessAgent, if logged on. 2. To use the Emergency Hot Key, unlock option must be set to 3. 3. Use of the Emergency Hot Key should be subject to proper behavior of auto-logoff from applications. 4. Use of the Emergency Hot Key should be subject to proper behavior of auto-logoff from applications. 	<p>[DO]</p> <p>"EmergencyHot-KeyEnabled"</p>	<p>Enable Emergency Hot Key?</p>	<p>#1: Yes</p> <p>*#0: No</p> <p>#True</p> <p>*#False</p> <p>(refreshed on startup)</p>	<p>Machine System</p>

pid_emergency_hot_key_sequence				
<p>The Emergency Hot Key sequence.</p> <p><i>Note:</i></p> <p>Effective only if Emergency Hot Key is enabled.</p>	<p>[DO]</p> <p>"EmergencyHot-KeySequence"</p>	<p>Emergency Hot Key sequence</p>	<p>*#Ctrl</p> <p>*#Alt</p> <p>*#End</p> <p>(max 3 keys from set of: Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E)</p> <p>(2 of the keys in this set should be used so that the probability of conflict with other applications is minimized: Ctrl, Shift, Alt)</p> <p>(refreshed on startup)</p>	<p>Machine System</p>

Presence detector policies				
pid_presence_detector_enabled				
<p>Whether presence detector is enabled.</p> <p><i>Note:</i></p> <p>This policy does not automatically enable or disable the third-party presence detector hardware and software.</p>	<p>[DO]</p> <p>"PresenceDetectorEnabled"</p>	<p>Enable presence detector?</p>	<p>#1: Yes</p> <p>*#0: No</p> <p>#True</p> <p>*#False</p> <p>(refreshed on startup)</p>	<p>Machine System</p>

Description	Registry	IMS Entry	Values	Scope
pid_presence_detector_walk_away_key_sequence				
<p>The key sequence that the presence detector will send when a user walks away from it.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <i>pid_presence_detector_enabled</i> is enabled. 2. The same key sequence should be configured on the presence detector by using third-party software. For RF IDEas <i>pcProx-Sonar</i>, configure the "Walk-away Keystrokes" using the <i>pcProx-Sonar Configuration Utility</i>. 	<p>[DO]</p> <p>"PresenceDetectorWalkAwayKeySequence"</p>	<p>Key sequence sent by presence detector when user walks away</p>	<p>*#Ctrl *#Alt *#PgDn</p> <p>(max 3 keys from set of: Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E)</p> <p>(2 of the keys in this set should be used so that the probability of conflict with other applications is minimized: Ctrl, Shift, Alt)</p> <p>(refreshed on startup)</p>	Machine System
pid_presence_detector_walk_away_action				
<p>Actions to be performed by AccessAgent when presence detector detects a user walking away while no user is logged on.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Effective only if <i>pid_presence_detector_enabled</i> is enabled. 2. Currently, this is supported only if <i>pid_lusm_sessions_max</i> = 1. In future, if <i>pid_lusm_sessions_max</i> > 1, AccessAgent with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen. 	<p>[DO]</p> <p>"PresenceDetectorWalkAwayAction"</p>	<p>Actions performed by AccessAgent when presence detector detects user walking away while no user is logged on</p>	<p>#0: No action #1: Log off Windows #2: Log off Wallet *#4: Lock computer #5: Log off Wallet and lock computer</p> <p>(refreshed on sync for system policy)</p> <p>(refreshed on use for machine policy)</p>	Machine System
pid_presence_detector_walk_away_action_countdown_secs				
<p>Confirmation countdown duration, in seconds, when presence detector detects a user walking away.</p> <p>Note:</p> <p>Effective only if <i>pid_presence_detector_enabled</i> is enabled.</p>	<p>[DO]</p> <p>"PresenceDetectorWalkAwayActionCountdownSecs"</p>	<p>Confirmation countdown duration, in seconds, when presence detector detects user walking away</p>	<p>*5</p> <p>(0 to disable confirmation countdown)</p> <p>(refreshed on sync for system policy)</p> <p>(refreshed on use for machine policy)</p>	Machine System

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

Configurable text policies

EnGINA text policies

pid_engina_welcome_text

Configurable text for EnGINA welcome message. <i>Notes:</i> 1. This message will be displayed, followed by a blank line, and then messages in one of the configurable text policies below (depending on second factors supported list). 2. Consecutive strings are separated by a blank line. 3. "\n\n" can be added if more blank lines are desired.		Welcome message (Maximum 2 lines)	*#This computer is protected by Encentuate AccessAgent. *#If you are here for the first time, click 'Sign up' to get started. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
---	--	-----------------------------------	---	--------

pid_engina_logon_with_pwd_text

Configurable text for password logon. <i>Note:</i> See pid_engina_welcome_text.		Instructions for password logon (Maximum 2 lines)	*#To log on, click 'Log on' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
--	--	---	---	--------

pid_engina_logon_with_rfid_text

Configurable text for RFID logon. <i>Note:</i> See pid_engina_welcome_text.		Instructions for RFID logon (Maximum 2 lines)	*#To log on, tap your RFID card. *#If you do not have your RFID card, click 'Log on' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
--	--	---	---	--------

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

pid_engina_logon_with_usb_key_text				
Configurable text for USB Key logon. <i>Note: See pid_engina_welcome_text.</i>		Instructions for USB Key logon (Maximum 2 lines)	<p>*#To log on, insert your Encentuate USB Key into the USB port now. If you have already inserted your Key and are not prompted for password, please remove your Key and insert it back again, or press Ctrl-Alt-Del.</p> <p>*#If you do not have your Encentuate USB Key, click 'Log on' or press Ctrl-Alt-Del.</p> <p>(2 strings max.)</p> <p>(text box takes 15 lines max, about 40 chars per line)</p> <p>(refreshed on sync)</p>	System

pid_engina_logon_with_arfid_text				
Configurable text for active proximity badge logon. <i>Note: See pid_engina_welcome_text.</i>		Instructions for active proximity badge logon (Maximum 2 lines)	<p>*#To log on, present your active proximity badge.</p> <p>*#To log on without active proximity badge, click 'Log on' or press Ctrl-Alt-Del.</p> <p>(2 strings max.)</p> <p>(text box takes 15 lines max, about 40 chars per line)</p> <p>(refreshed on sync)</p>	System

pid_engina_logon_with_fingerprint_text				
Configurable text for fingerprint logon. <i>Note: See pid_engina_welcome_text.</i>		Instructions for fingerprint logon (Maximum 2 lines)	<p>*#To log on, place your registered finger on the sensor.</p> <p>*#To log on without fingerprint, click 'Log on' or press Ctrl-Alt-Del.</p> <p>(2 strings max.)</p> <p>(text box takes 15 lines max, about 40 chars per line)</p> <p>(refreshed on sync)</p>	System

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

pid_engina_logon_with_fingerprint_or_rfid_text				
Configurable text for fingerprint or RFID logon. <i>Note: See pid_engina_welcome_text.</i>		Instructions for fingerprint or RFID logon (Maximum 2 lines)	*#To log on, place your registered finger on the sensor or tap your RFID card. *#To log on without fingerprint or RFID card, click 'Log on' or press Ctrl-Alt-Del. (2 strings max) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

pid_logon_credentials_text				
Configurable text that is to be displayed right above the logon credentials when user clicks on 'Log on'. <i>Note:</i> <i>If pid_enc_pwd_is_ad_pwd_enabled is set to True, this policy should be modified accordingly, for example, "Enter your Windows domain user name and password to log on."</i>		Logon credentials message (Maximum 1 line)	*#Enter your user name and password to log on. (1 string max.) (text box takes 2 lines max, about 40 chars per line) (refreshed on sync)	System

Unlock text policies				
pid_unlock_text				
Configurable text for computer locked message. <i>Notes:</i> 1. This message will be displayed, followed by a blank line, and then messages in one of the configurable text policies below (depending on current Wallet and pid_unlock option). 2. Consecutive strings are separated by a blank line. 3. "\n\n" can be added if more blank lines are desired.		Locked computer message (Maximum 1 line)	*#This computer is protected by Encentuate AccessAgent, and has been locked. (1 string max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_unlock_with_pwd_option_1_text				
Configurable text for unlocking with password when computer locked and pid_unlock option is 1. <i>Note: See pid_unlock text.</i>		Instructions for unlocking with password when unlock policy is 'only the same user can unlock' (Maximum 2 lines)	*#To unlock, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_pwd_option_3_text				
Configurable text for unlocking with password when computer locked and pid_unlock option is 3. <i>Note: See pid_unlock text.</i>		Instructions for unlocking with password when unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)	*#To unlock, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_pwd_option_4_text				
Configurable text for unlocking with password when computer locked and pid_unlock_option is 4. <i>Note: See pid_unlock_text.</i>		Instructions for unlocking with password when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)	*#To unlock, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max) (textbox takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_unlock_with_usb_key_option_1_text				
Configurable text for unlocking with USB Key when computer locked and pid_unlock option is 1. <i>Note: See pid_unlock text.</i>		Instructions for unlocking with USB Key when unlock policy is 'only the same user can unlock' (Maximum 2 lines)	<p>*#To unlock, insert your Encentuate USB Key into the USB port now. If you have already inserted your Key and are not prompted for password, please remove your Key and insert it back again, or press Ctrl-Alt-Del.</p> <p>*#If you do not have your Encentuate USB Key, click 'Unlock this computer' or press Ctrl-Alt-Del.</p> <p>(2 strings max.)</p> <p>(text box takes 15 lines max, about 40 chars per line)</p> <p>(refreshed on sync)</p>	System
pid_unlock_with_usb_key_option_3_text				
Configurable text for unlocking with USB Key when computer locked and pid_unlock_option is 3. <i>Note: See pid_unlock text.</i>		Instructions for unlocking with USB Key when unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)	<p>*#To unlock, insert your Encentuate USB Key into the USB port now. If you have already inserted your Key and are not prompted for password, please remove your Key and insert it back again, or press Ctrl-Alt-Del.</p> <p>*#If you do not have your Encentuate USB Key, click 'Unlock this computer' or press Ctrl-Alt-Del.</p> <p>(2 strings max.)</p> <p>(text box takes 15 lines max, about 40 chars per line)</p> <p>(refreshed on sync)</p>	System

Description	Registry	IMS Entry	Values	Scope
pid_unlock_with_usb_key_option_4_text				
Configurable text for unlocking with USB Key when computer locked and pid_unlock option is 4. <i>Note: See pid_unlock text.</i>		Instructions for unlocking with USB Key when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)	<p>*#To unlock, insert your Encentuate USB Key into the USB port now. If you have already inserted your Key and are not prompted for password, please remove your Key and insert it back again, or press Ctrl-Alt-Del.</p> <p>*#If you do not have your Encentuate USB Key, click 'Unlock this computer' or press Ctrl-Alt-Del.</p> <p>(2 strings max)</p> <p>(textbox takes 15 lines max, about 40 chars per line)</p> <p>(refreshed on sync)</p>	System
pid_unlock_with_rfid_option_1_text				
Configurable text for unlocking with RFID when computer locked and pid_unlock option is 1. <i>Note: See pid_unlock text.</i>		Instructions for unlocking with RFID when unlock policy is 'only the same user can unlock' (Maximum 2 lines)	<p>*#To unlock, tap your RFID card.</p> <p>*#If you do not have your RFID card, click 'Unlock this computer' or press Ctrl-Alt-Del.</p> <p>(2 strings max.)</p> <p>(text box takes 15 lines max, about 40 chars per line)</p> <p>(refreshed on sync)</p>	System
pid_unlock_with_rfid_option_3_text				
Configurable text for unlocking with RFID when computer locked and pid_unlock_option is 3. <i>Note: See pid_unlock text.</i>		Instructions for unlocking with RFID when unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)	<p>*#To unlock, tap your RFID card.</p> <p>*#If you do not have your RFID card, click 'Unlock this computer' or press Ctrl-Alt-Del.</p> <p>(2 strings max.)</p> <p>(text box takes 15 lines max, about 40 chars per line)</p> <p>(refreshed on sync)</p>	System

Description	Registry	IMS Entry	Values	Scope
pid_unlock_with_rfid_option_4_text				
Configurable text for unlocking with RFID when computer locked and pid_unlock_option is 4. <i>Note: See pid_unlock text.</i>		Instructions for unlocking with RFID when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)	*#To unlock, tap your RFID card. *#If you do not have your RFID card, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max) (textbox takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_arfid_option_1_text				
Configurable text for unlocking with active proximity badge when computer locked and pid_unlock_option is 1. <i>Note: See pid_unlock text.</i>		Instructions for unlocking with active proximity badge when unlock policy is 'only the same user can unlock' (Maximum 2 lines)	*#To unlock, present your active proximity badge. *#To unlock without active proximity badge, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_arfid_option_3_text				
Configurable text for unlocking with active proximity badge when computer locked and unlock option is 3. <i>Note: See pid_unlock text.</i>		Instructions for unlocking with active proximity badge when unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)	*#To unlock, present your active proximity badge. *#To unlock without active proximity badge, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

pid_unlock_with_arfid_option_4_text				
Configurable text for unlocking with active proximity badge when computer locked and pid_unlock_option is 4. <i>Note: See pid_unlock_text.</i>		Instructions for unlocking with active proximity badge when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)	*#To unlock, present your active proximity badge. *#To unlock without active proximity badge, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max) (textbox takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

pid_unlock_with_fingerprint_option_1_text				
Configurable text for unlocking with fingerprint when computer locked and unlock option is 1. <i>Note: See pid_unlock_text.</i>		Instructions for unlocking with fingerprint when unlock policy is 'only the same user can unlock' (Maximum 2 lines)	*#To unlock, place your registered finger on the sensor. *#To unlock without fingerprint, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

pid_unlock_with_fingerprint_option_3_text				
Configurable text for unlocking with fingerprint when computer locked and unlock option is 3. <i>Note: See pid_unlock_text.</i>		Instructions for unlocking with fingerprint when unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)	*#To unlock, place your registered finger on the sensor. *#To unlock without fingerprint, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_unlock_with_fingerprint_option_4_text				
Configurable text for unlocking with fingerprint when computer locked and pid_unlock_option is 4. <i>Note: See pid_unlock_text.</i>		Instructions for unlocking with fingerprint when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)	*#To unlock, place your registered finger on the sensor. *#To unlock without fingerprint, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max) (textbox takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_fingerprint_or_rfid_option_1_text				
Configurable text for unlocking with fingerprint or RFID when computer locked and pid_unlock_option is 1. <i>Note: See pid_unlock_text.</i>		Instructions for unlocking with fingerprint or RFID when unlock policy is 'only the same user can unlock' (Maximum 2 lines)	*#To unlock, place your registered finger on the sensor or tap your RFID card. *#To unlock without fingerprint or RFID card, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_fingerprint_or_rfid_option_3_text				
Configurable text for unlocking with fingerprint or RFID when computer locked and pid_unlock_option is 3. <i>Note: See pid_unlock_text.</i>		Instructions for unlocking with fingerprint or RFID when unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)	*#To unlock, place your registered finger on the sensor or tap your RFID card. *#To unlock without fingerprint or RFID card, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

pid_unlock_with_fingerprint_or_rfid_option_4_text				
Configurable text for unlocking with fingerprint or RFID when computer locked and pid_unlock_option is 4. <i>Note: See pid_unlock_text.</i>		Instructions for unlocking with fingerprint or RFID when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)	*#To unlock, place your registered finger on the sensor or tap your RFID card. *#To unlock without fingerprint or RFID card, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

pid_unlock_credentials_text				
Configurable text that is to be displayed right above the unlock credentials when user clicks on 'Unlock this computer'. <i>Note: If Encentuate password is AD password is set to True, this policy should be modified accordingly, for example, "Enter your Windows domain user name and password to unlock".</i>		Unlock credentials message (Maximum 1 line)	*#Enter your user name and password to unlock. (1 string max.) (text box takes 2 lines max, about 40 chars per line) (refreshed on sync)	System

RFID text policies				
---------------------------	--	--	--	--

pid_rfid_name_text				
Configurable text for RFID name, for example, 'RFID card'.		RFID name	*RFID card (refreshed on sync)	System

Sign up text policies				
------------------------------	--	--	--	--

pid_bind_display_template				
The template to be used for displaying the sign-up dialog. <i>Notes:</i> 1. The Domain field is also shown if and only if the enterprise directory is AD. 2. Other than the domain, the template can only support either 1 or 2 fields. To display only one field, set the Label of one of the fields to a blank entry. The field with the blank Label will not be displayed.		Template for sign-up dialogBind template*	#Enter your domain user name and password for identity verification. *#User name *#Password (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

AccessAssistant and Web Workplace text policies

pid_accessanywhere_otp_reset_link_text

Configurable text for the OTP (OATH) reset link on AccessAssistant and Web Workplace. <i>Note: Effective only if pid_auth_authentication_option for "AccessAnywhere" contains "OTP (OATH)".</i>		Text for the OTP (OATH) reset link on AccessAssistant and Web Workplace.	*Reset OTP token (refreshed on sync)	System
--	--	--	---	--------

Authentication Service policies

Password policies

pid_auth_reauth_with_enc_pwd_enabled

Whether Encentuate password re-authentication is required before performing automatic sign-on for the authentication service. <i>Note: Effective only if "authentication is enterprise" is enabled for the authentication service.</i>		Require re-authentication before performing automatic sign-on?	#True *#False (refreshed on sync)	System
---	--	--	---	--------

pid_auth_pwd_is_ad_pwd

Whether the authentication service is displayed as a Windows user account in AccessAdmin.		Is the password the Windows logon password?	#True *#False (refreshed on use)	System
---	--	---	--	--------

pid_auth_fortification_pwd_min_length

Minimum length of an acceptable password for the authentication service. <i>Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.</i>		Minimum password length	*6 (from 1 to 99) (refreshed on sync)	System
---	--	-------------------------	---	--------

pid_auth_fortification_pwd_max_length

Maximum length of an acceptable password for the authentication service. <i>Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.</i>		Maximum password length	*20 (from 1 to 99) (refreshed on sync)	System
---	--	-------------------------	--	--------

Description	Registry	IMS Entry	Values	Scope
pid_auth_fortification_pwd_min_numerics_length				
Minimum number of numeric characters for an acceptable password for the authentication service. <i>Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.</i>		Minimum number of numeric characters	*0 (from 0 to 99) (refreshed on sync)	System
pid_auth_fortification_pwd_min_alphabets_length				
Minimum number of alphabetic characters for an acceptable password for the authentication service. <i>Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.</i>		Minimum number of alphabetic characters	*0 (from 0 to 99) (refreshed on sync)	System
pid_auth_fortification_pwd_min_special_chars_length				
Minimum number of special characters for an acceptable password for the authentication service. <i>Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.</i>		Minimum number of special characters	*0 (from 0 to 99) (refreshed on sync)	System
pid_auth_fortification_pwd_max_numerics_length				
Maximum number of numeric characters for an acceptable password for the authentication service. <i>Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.</i>		Maximum number of numeric characters	*10 (from 0 to 99) (0 for no max limit) (refreshed on sync)	System
pid_auth_fortification_pwd_max_alphabets_length				
Maximum number of alphabetic characters for an acceptable password for the authentication service. <i>Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.</i>		Maximum number of alphabetic characters	*10 (from 0 to 99) (0 for no max limit) (refreshed on sync)	System
pid_auth_fortification_max_special_chars_length				
Maximum number of special characters for an acceptable password for the authentication service. <i>Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.</i>		Maximum number of special characters	*10 (from 0 to 99) (0 for no max limit) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_auth_fortification_pwd_mixed_case_enforced				
Whether to enforce the use of both upper case and lower case characters for the password of the authentication service. <i>Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.</i>		Enforce the use of both upper case and lower case characters?	#True *#False (refreshed on sync)	System
pid_auth_fortification_random_pwd_enabled				
Whether manual password change with random password is enabled for the authentication service.		Enable manual password change with random password?	#True *#False (refreshed on sync)	User
Authentication policies				
pid_auth_is_enterprise				
Whether an authentication service is an enterprise authentication service.		Is it an enterprise authentication service?	#True *#False (refreshed on sync)	System
pid_auth_inject_pwd_entry_option_default				
Default automatic sign-on password entry option for the authentication service. <i>Notes:</i> 1. <i>Effective only if "authentication is enterprise" is enabled for the authentication service.</i> 2. <i>Overrides Wallet inject password entry option default.</i>		Default automatic sign-on password entry option for the authentication service	#1: Automatic logon *#2: Always #3: Ask #4: Never #5: Certificate #6: Use application settings (refreshed on sync)	System
pid_auth_sso_enabled				
Whether to enable automatic sign-on for the authentication service. <i>Note: Effective only if "authentication is enterprise" is enabled for the authentication service.</i>		Enable automatic sign-on?	*#True #False (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

* pid_auth_authentication_option				
<p>Option to control what authentication modes AccessAgent should support for the authentication service.</p> <p><i>Note: Effective only if "authentication is enterprise" is enabled for the authentication service.</i></p>		Authentica- tion modes to be supported	*#1: Password #2: SCR #4: CAPI #8: OTP #16: MAC #32: CCOW (multiple allowed) (refreshed on sync)	System

pid_auth_accounts_max				
<p>Maximum number of accounts that user can store for the authentication service.</p> <p>Notes:</p> <p>1. When the number of accounts has reached or exceeded the maximum specified by this policy:</p> <p>a) AccessAgent does not capture any-more new accounts for this authentication service.</p> <p>b) If user clicks on "Add new user" button in Wallet Manager, AccessAgent prompts that the number of accounts has reached the limit.</p> <p>2. User policy, if defined, overrides system policy.</p>		Maximum number of accounts allowed for the authenti- cation service	*0 (from 0 to 10) (0 for no max limit) (refreshed on sync)	User System

pid_auth_capture_prompt_enabled				
<p>Whether user should be prompted during auto-capture of password for the authentication service.</p> <p>Notes:</p> <p>1. Effective only if pid_auth_is_enterprise is enabled for the authentication service.</p> <p>2. In the case of policy value False, if some user is already logged on and another user wants to use the computer for some time, the second user's application passwords may be auto-captured into the first user's Wallet. Hence, if pid_auth_capture_prompt_enabled is set to False for an authentication service, it is recommended that pid_auth_account_max be set to 1 for the same authentication service.</p>		Prompt user on auto-cap- ture of pass- word?	*#True #False (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
-------------	----------	-----------	--------	-------

User-defined policies

pid_auth_inject_pwd_entry_option

<p>Password entry of injection policy per authentication service.</p>			<p>#1: Automatic logon</p> <p>*#2: Always</p> <p>#3: Ask</p> <p>#4: Never</p> <p>#5: Certificate</p> <p>#6: Use application settings (refreshed on use)</p>	User
---	--	--	---	------

pid_auth_inject_user_default

<p>Default user of injection policy per authentication service.</p>			(refreshed on use)	User
---	--	--	--------------------	------

Application policies

pid_app_authentication_option

<p>Option to control what authentication modes AccessAgent should support for the application.</p>		<p>Authenticat- tion modes to be supported</p>	<p>*#1: Password</p> <p>#2: SCR</p> <p>#4: CAPI</p> <p>#8: OTP</p> <p>#16: MAC (multiple allowed) (refreshed on sync)</p>	System
--	--	--	---	--------

pid_app_reauth_with_enc_pwd_enabled

<p>Whether Encentuate password re-authentication is required before performing automatic sign-on for the application.</p> <p><i>Note: Overrides authenticate/re-authenticate with Encentuate password.</i></p>		<p>Require re-authenticat- ion before performing automatic sign-on?</p>	<p>#True</p> <p>*#False (refreshed on sync)</p>	System
--	--	---	---	--------

pid_app_inject_pwd_entry_option_default

<p>Default automatic sign-on password entry option for the application.</p> <p><i>Note: Overrides authentication inject password entry option default and Wallet inject password entry option default.</i></p>		<p>Default auto- matic sign-on password entry option for the appli- cation</p>	<p>#1: Automatic logon</p> <p>*#2: Always</p> <p>#3: Ask</p> <p>#4: Never</p> <p>#5: Certificate</p> <p>#6: Use application settings (refreshed on sync)</p>	System
--	--	--	--	--------

Description	Registry	IMS Entry	Values	Scope
pid_app_wallet_logoff_action				
<p>Action to take for the application when user logs off AccessAgent.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This policy overrides Wallet logoff action for applications default. 2. Please see the notes for Wallet logoff action for applications default. 3. For web applications, each URL is considered an application. Internet Explorer (IE) is also considered an application. In this context, the web application policy overrides the IE policy, which overrides Wallet logoff action for applications default. 4. Recommended settings for IE and Windows Explorer: 2 and 3 respectively. 5. This policy is set to 3 for Windows logon (application GINA) when IMS is installed. 		Action for the application, when user logs off AccessAgent	<p>#1: Log off the application</p> <p>#2: Close the application</p> <p>*#3: Do nothing (refreshed on sync)</p>	System

User-defined policies

pid_app_auth_inject_pwd_entry_option				
Password entry of injection policy per application per authentication service.			<p>#1: Automatic logon</p> <p>*#2: Always</p> <p>#3: Ask</p> <p>#4: Never</p> <p>#5: Certificate</p> <p>#6: Use application settings (refreshed on use)</p>	User
pid_app_auth_inject_user_default				
Default user of injection policy per application per authentication service.			(refreshed on use)	User

Troubleshooting

pid_wallet_sync_manual_enabled				
Whether to enable a "Synchronize with IMS" option by right-clicking AA in WNA.	[T] "WalletSyncManualEnabled"		<p>*#0: No</p> <p>#1: Yes (refreshed on use)</p>	Machine

Description	Registry	IMS Entry	Values	Scope
pid_wallet_delete_enabled				
<p>Whether to enable a "Delete user Wallets" option by right-clicking AA in WNA.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This menu item is only available when no user is logged on to AA. 2. This menu item deletes all user Wallets, but not the machine Wallet. 3. If this feature is to be used on a Citrix or Terminal Server or a workstation with Local User Session Management (LUSM) enabled, make sure that only one desktop session is running while deleting the Wallets. If multiple sessions are running, the behavior of AA in other sessions after deleting the Wallets is unpredictable. 	<p>[T]</p> <p>"WalletDeleteEnabled"</p>		<p>*#0: No</p> <p>#1: Yes</p> <p>(refreshed on use)</p>	Machine
pid_machine_policy_override_enabled				
<p>Whether to override machine policies using registry values.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If enabled, machine policies can be overridden for this machine by specifying their values in the registry key [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\DeploymentOptions]. E.g., <code>pid_second_factors_supported_list</code> can be specified using the registry value "SecondFactorsSupportedList". 2. This temporary policy is useful for troubleshooting, especially if there is no administrator access to IMS Server. Please remember to disable this policy after testing is completed, so that the machine can continue to be managed through AccessAdmin. 	<p>[T]</p> <p>"MachinePolicyOverrideEnabled"</p>		<p>*#0: No</p> <p>#1: Yes</p> <p>(refreshed on use)</p>	Machine

Encentuate IMS Bridge for Citrix

The Encentuate IMS Bridge for Citrix is not a standard product component. The bridge must be customized by Professional Services for each deployment. The bridge integrates with the Citrix web interface (Web Interface) and handles user authentication for the Citrix Web Interface server.

When a user tries to logon to the Citrix Web Interface server, the Encentuate IMS bridge intercepts the request and may redirect the authentication to the IMS Server, if necessary. The user interface and protocol can be different for each deployment.

Below are some of the possible deployment options:

- The user enters the Encentuate user name and password, which are verified at the IMS Server. The IMS Bridge then gets the user's ActiveDirectory (AD) logon user name and password from the user's Wallet on the IMS Server and redirects the authentication to the Citrix MetaFrame server with the Active Directory logon user name and password.
- The user enters the Encentuate user name and password, which are verified at the IMS Server. Subsequently, the IMS Bridge prompts the user to enter a One-Time Password (OTP) or Mobile Access Code (MAC) for additional verification. After second factor authentication, only the IMS Bridge gets the Active Directory user name and password from the user's Wallet on the IMS Server and redirects the authentication to MetaFrame server.



When the user tries to log on to the web interface from the office/Intranet environment (AccessAgent is running a local computer), it may be inconvenient to send to the user's mobile phone. For such cases, use AccessAgent to generate an OTP and include it in the web logon form as a hidden field. The IMS Bridge verifies the OTP from the hidden field and avoids sending an MAC to the user's mobile phone.

- The user may first enter an Active Directory user name and password, which are verified at the Active Directory server. The IMS Bridge can then prompt the user for second factor authentication (e.g., OTP or MAC).

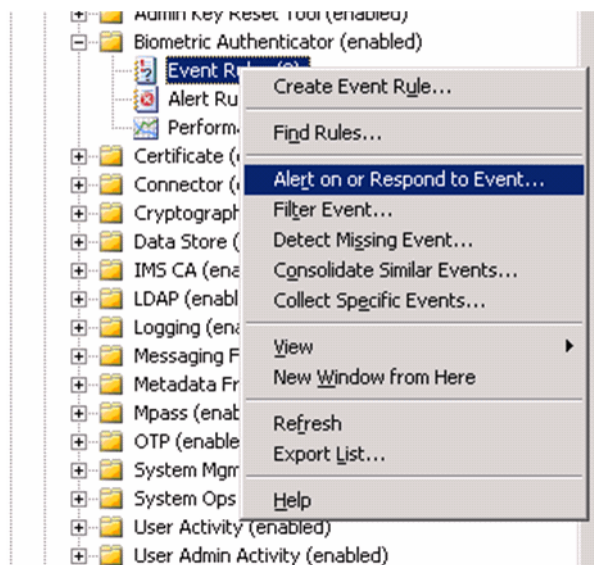
- The IMS Bridge can support additional functions to update Active Directory password changes in the user's Wallet on the IMS Server. If the Active Directory password expires, the user must change the Active Directory password through the web interface. The user can also manually change the Active Directory password from the web interface. For both cases, the IMS Bridge can capture the new Active Directory password and updates the user's Wallet at the IMS Server.

Creating a rule in MOM

The MOM Management Pack for IMS Server already contains all the rules needed for a typical deployment. To add more rules, go through the following procedure to create a new alert rule for IMS Server events.

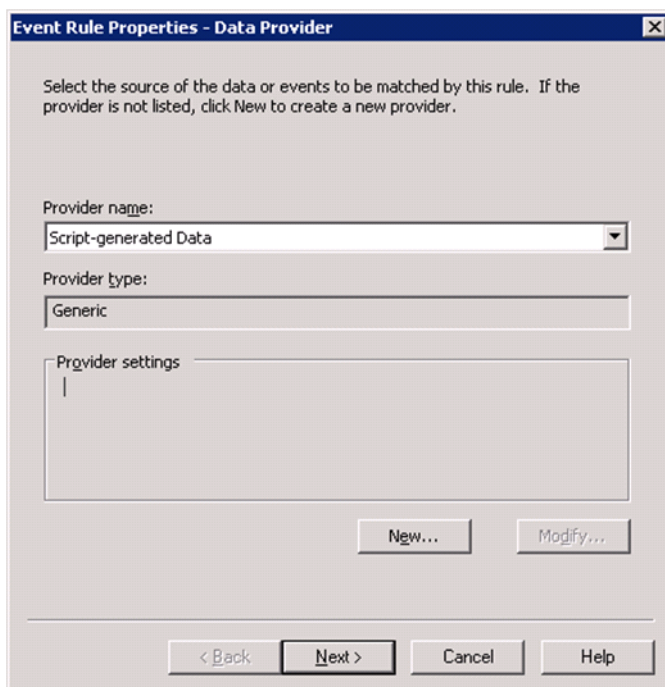
To create a new alert rule:

- ❶ Select the folder related to the alert being created.
- ❷ Right-click on **Event Rules**.
- ❸ Select the appropriate type for the rule. In this example, **Alert on or Respond to Event** is chosen.



Alert of responding to events

- ❹ Select **Script-generated Data** as the provider name.



Event Rule Properties - Data Provider

Select the source of the data or events to be matched by this rule. If the provider is not listed, click New to create a new provider.

Provider name:
Script-generated Data

Provider type:
Generic

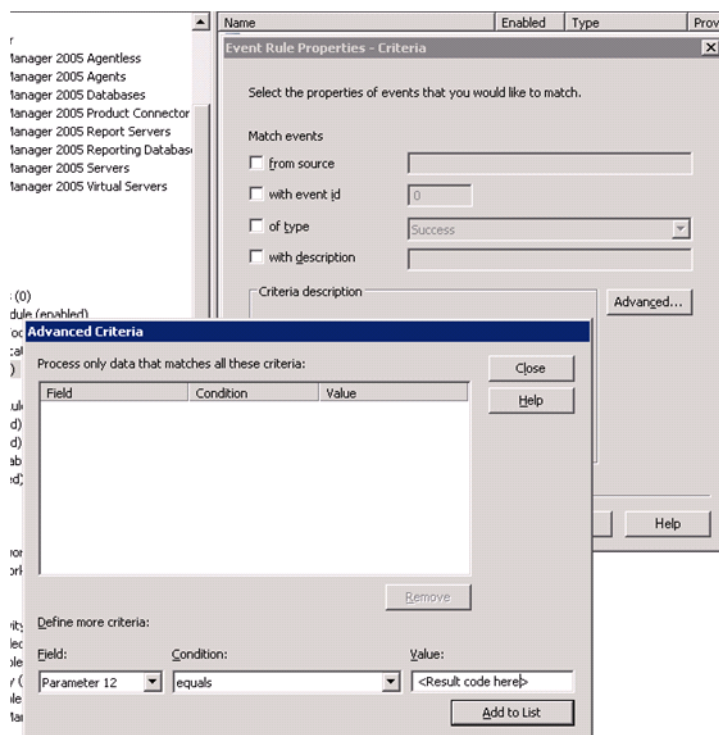
Provider settings

New... Modify...

< Back Next > Cancel Help

Event Rule Properties window

- 5 Click **Next**.
- 6 Click **Advanced**.



Advanced Criteria

Process only data that matches all these criteria:

Field	Condition	Value
Parameter 12	equals	<Result code here>

Define more criteria:

Field: Condition: Value:

Parameter 12 equals <Result code here>

Add to List

Remove

Close Help

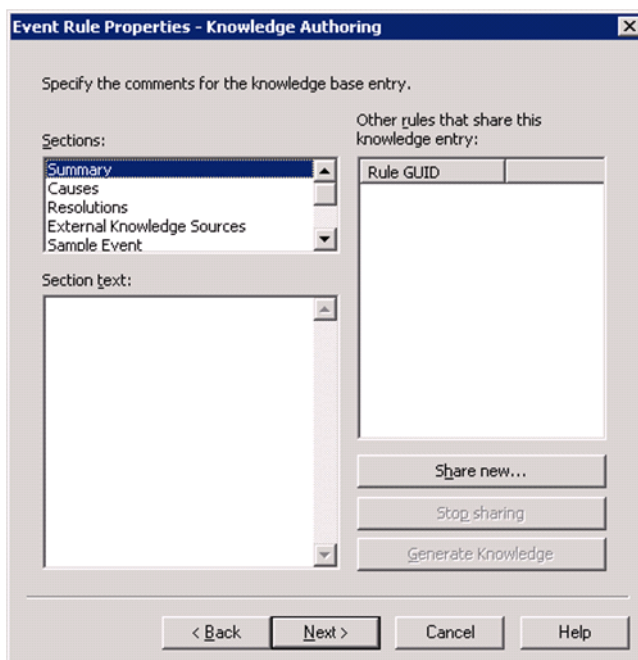
Advanced...

Advanced Event Rule Criteria

- 7 Select **Parameter 12** from the **Field** drop down list (**Parameter 12** refers to Result Code). For parameter mapping, refer to [Mapping MOM Log Parameters to IMDS Server Log Attributes](#).
- 8 In the **Value** field, enter the result code in integer format (not Hexadecimal).
- 9 For more precise event monitoring, include the Event Code or other parameters.
- 10 Click **Add to list** and close the current window.
- 11 Click **Next** in the Event rule properties - Criteria window.
- 12 In the Alert window, select the **Alert severity** and enter any custom message.

Alert window

- 13 Click **Next** up to Knowledge Authoring.
- 14 Create product knowledge for the alert. Knowledge should be written in HTML format (if this window cannot be found, move on to the next).



Event Rule Properties - Knowledge Authoring

Specify the comments for the knowledge base entry.

Sections:

- Summary
- Causes
- Resolutions
- External Knowledge Sources
- Sample Event

Section text:

Other rules that share this knowledge entry:

Rule GUID

Share new...

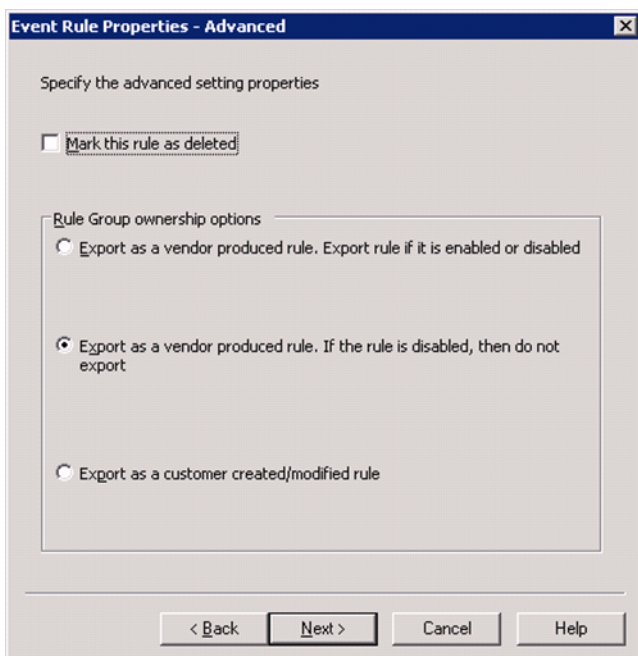
Stop sharing

Generate Knowledge

< Back Next > Cancel Help

Knowledge Authoring window

- 15 Select either the first or second option. The second option is preferred.



Event Rule Properties - Advanced

Specify the advanced setting properties

☐ Mark this rule as deleted

Rule Group ownership options

- ☐ Export as a vendor produced rule. Export rule if it is enabled or disabled
- ☒ Export as a vendor produced rule. If the rule is disabled, then do not export
- ☐ Export as a customer created/modified rule

< Back Next > Cancel Help

Event Rule Properties - Advanced window

- 16 Click **Next** to continue.
- 17 Enter a **Rule Name**.

Event Rule Properties - General

Rule Name:

Rule action:

Rule GUID:

☒ This rule is enabled

☐ Enable rule-disable overrides for this rule

Override Name:

No override criteria have been set

Note: Changing the override name assigns a new override to this rule property. Override criteria set for the previous override name will no longer apply to this rule.

Event Rule Properties - General window

- 18 Click **Finish**.

Testing Redirection of COM Port

This section covers the following topics:

- [Pre-requisites](#)
- [Running the check](#)



If the outlined steps do not work, you can alternatively use the net use command on the remote server to verify if COM redirection happens. After the command is entered, you should see an entry similar to "COM1 is mapped to \\Client\COM1" if the configuration is correct.

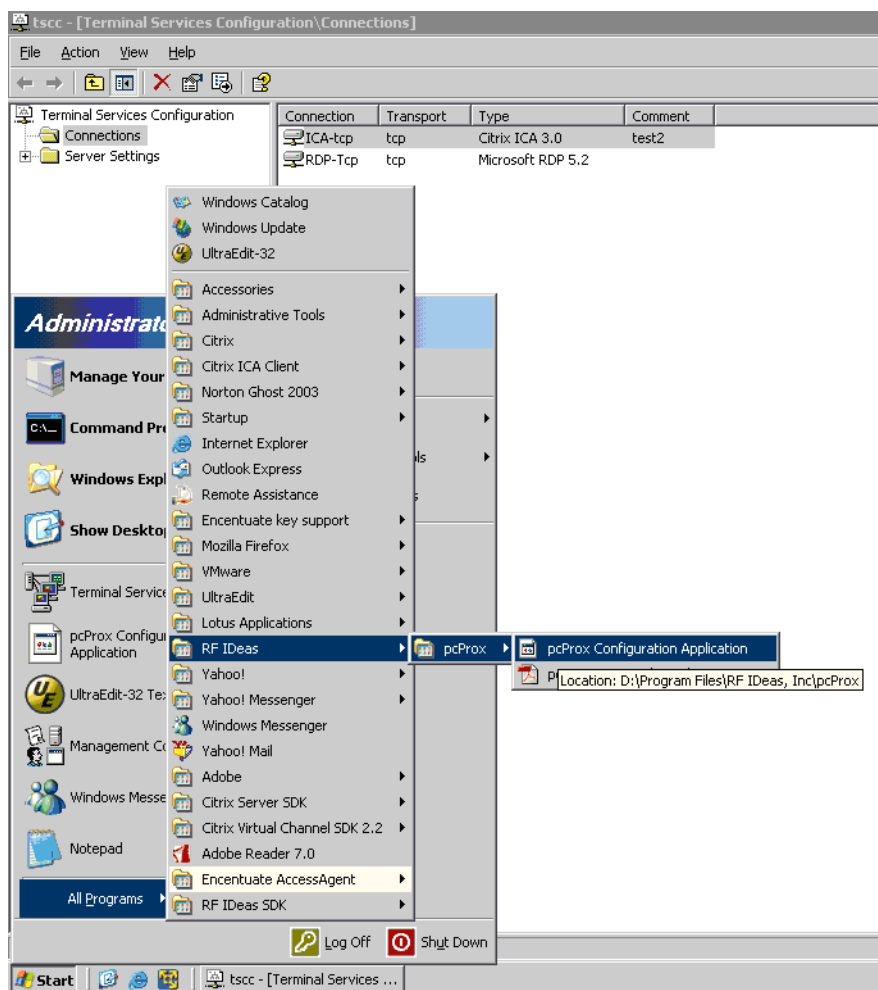
Prerequisites

To verify that the configuration settings have been applied successfully, you must have a Windows CE Thin Client connecting to the server through an ICA/RDP session.

Ensure that the RFIDEas pcProx Configuration Application has been installed on the server.

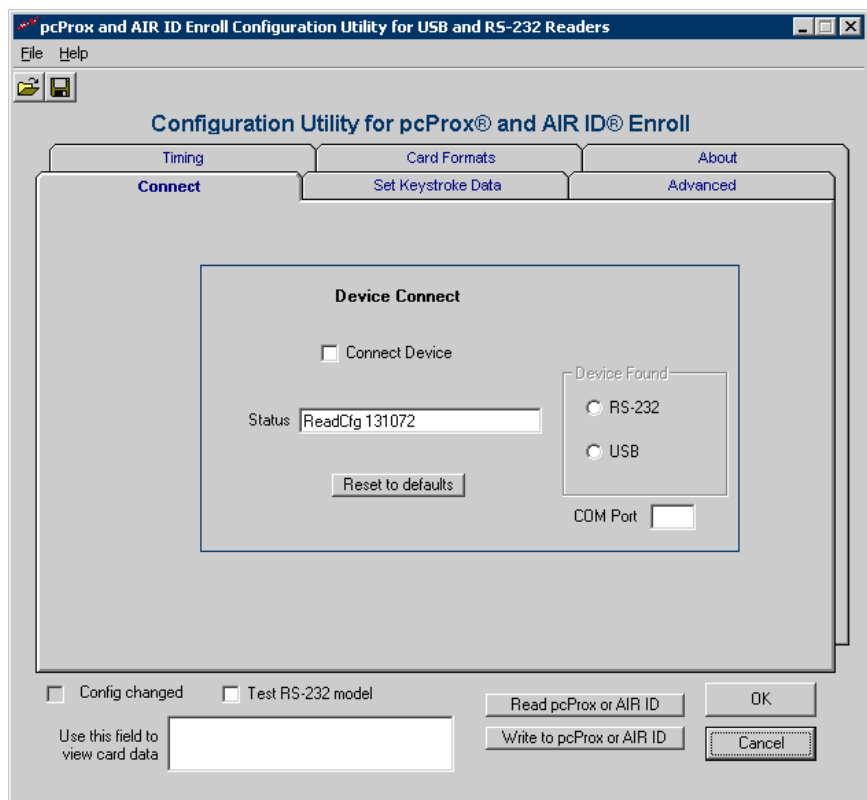
Running the check

- 1 Once the pcProx application has been installed on the Server, using a Thin Client with the RFIDEas RS232 reader connected, start an RDP/ICA Session with the Server.
- 2 Once the session has started, start the pcProx Configuration Application by clicking on *Start >> All Programs >> RF Ideas >> pcProx >> pcProx Configuration Application*.



Start the pcProx Configuration Application

- ③ An UNSUCCESSFUL configuration dialog box is displayed. Click **OK**.
- ④ A SUCCESSFUL configuration shows the following window.



Configure and click OK.

Once the settings have been confirmed as successful, close the pcProx windows application and install AccessAgent.

Mapping MOM Log Parameters to IMDS Server Log Attributes

This section covers the following MOM log tables:

- [IMSLOGSystemOps](#)
- [IMSLOGUserActivity](#)
- [IMSLOGUserService](#)
- [IMSLOGUserAdminActivity](#)
- [IMSLOGSystemMgmtActivity](#)

IMSLOGSystemOps

MOM Log Parameter No.	IMS Server Log Attribute
2	logId
3	LogImsServerId
4	caller
5	logLevel
6	message
7	stackTrace
8	serverMachine
9	logHash
10	logSign
11	logTime

IMSLOGUserActivity

|

MOM Log Parameter No.	IMS Server Log Attribute
2	logId
3	logImsServerId
4	imsId
5	socId
6	clientIpAddr
7	appld
8	appUid
9	description
10	serverMachine
11	resultCode
12	eventCode
13	logHash
14	logSign
15	logTime
16	enterpriseld
17	sociType
18	authenticatorType

IMSLOGUserService

MOM Log Parameter No.	IMS Server Log Attribute
2	logId
3	logImsServerId
4	imsId
5	socId
6	clientIpAddr
7	serverMachine
8	logHash
9	logSign
10	logTime
11	resultCode
12	eventCode

MOM Log Parameter No.	IMS Server Log Attribute
13	enterpriseld
14	sociType
15	authenticatorType

IMSLOGUserAdminActivity

MOM Log Parameter No.	IMS Server Log Attribute
2	logId
3	logImsServerId
4	adminImsId
5	adminSocId
6	authType
7	clientIpAddr
8	userImsId
9	userSocId
10	serverMachine
11	resultCode
12	eventCode
13	logHash
14	logSign
15	logTime
16	adminEntId
17	adminSociType
18	adminAuthType
19	userEntId
20	userSocId
21	userAuthType
22	authTypeDesc

IMSLOGSystemMgmtActivity

MOM Log Parameter No.	IMS Server Log Attribute
2	logId
3	logImsServerId
4	adminImsId
5	adminSocId
6	authType
7	clientIpAddr
8	serverMachine
9	logHash
10	logSign
11	resultCode
12	eventCode
13	logTime

Device Monitoring-Related Registry Entries

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\SOCIMonitor:

Value: MapRemoteClientComPortEnabled

Type: DWORD

Default Value: 1 (enabled)

Allowed Values: 1 (enabled), 0 (disabled)

Description: This value indicates whether the device monitoring mechanism should perform com port redirection from the client machine (connecting to the TS Server) to the TS server.

Value: LocalVirtualComPort

Type: DWORD

Default Value: 1

Range: [1, 8]

Description: This value indicates the virtual com port on the server where the data from the client com port is redirected.

Value: RemoteClientComPort

Type: DWORD

Default Value: 1

Range: [1, * (depending upon how many physical com ports are present on the client)]

Description: This value indicates the physical com port on the client (thin) where the reader (RFID) is connected. The redirection will take place from this port to the server's virtual com port configured in the registry value `LocalVirtualComPort`.

Shared Workstation & Monitoring-Related Registry Entries

The following are registry values recommended for the Thin Client demo:

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\DeploymentOptions]
```

```
"MachineTypeTS"=dword:00000001
```

```
"TSEnginaLogonNoLocalSessionEnabled"=dword:00000000
```

```
"TSWalletCachingOption"=dword:00000002
```

```
"TSLogonCacheEnabled"=dword:00000000
```

```
"TSLogonPromptEnabled"=dword:00000000
```

```
"UnlockWithWinOption"=dword:00000002
```

```
"UnlockOption"=dword:00000003
```

```
"EnginaWinlogonOptionEnabled"=dword:00000001
```

```
"UnlockDifferentUserAction"=dword:00000000
```

```
"RfidOnlyUnlockTimeoutSecs"=dword:00000300
```

```
"RfidTapSameAction"=dword:00000004
```

```
"RfidTapSameActionCountdownSecs"=dword:00000005
```

```
"RfidOnlyUnlockEnabled"=dword:00000001
```

```
"LogonUserNamePrefillOption"=dword:00000000
```

```
"WinStartupAction"=dword:00000001
```

```
"RfidTapDifferentActionCountdownSecs"=dword:00000005
```

"RfidTapDifferentAction"=dword:00000006

"SecondFactorsSupportedList"=RFID

[HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\SOCIMonitor]

"LocalVirtualComPort"=dword:00000001

"RemoteClientComPort"= the physical port number that the reader is connected to the Thin Client

"MapRemoteClientComPortEnabled"=dword:00000001

VBScript for Registering and Starting ObsService

The following are registry values recommended for the Thin Client demo:

```
'-----8<-----  
' This script registers and starts ObsService  
'  
' Expects ObsService.exe to be present in the  
' Encentuate Install Folder  
'  
' After execution check from services msc  
' whether service is started  
'  
' suhail@encentuate.com  
'-----8<-----
```

```
Set oShell = CreateObject("WScript.Shell")
```

```
progdir =  
(oShell.RegRead("HKLM\SOFTWARE\Encentuate\ProgramDir"))
```

```
ObsServiceExe = progdir + "ObsService.exe"
```

```
msgbox "Going to register " + ObsServiceExe + " as a service"
```

```
oShell.Exec(ObsServiceExe + " /service")
```

```
oShell.Exec("net start ObsService")
```

```
WScript.Quit
```

```
'-----8<-----
```


Configuring Auto-Logon to Servers

This section covers the following topics:

- [Configuring auto-logon for RDP clients](#)
- [Configuring auto-logon for ICA clients](#)

Configuring auto-logon for RDP clients

Verify that the following configurations are done on the TS/Citrix server:

- ❶ In Winlogon registry hive, `GinaDLL=enGINA.dll`.
- ❷ In Encentuate DO registry hive, `TSEngineLogonNoLocalSessionEnabled=0`

With these two registries set, the Welcome screen will show msGINA's Welcome screen (or other GINA if there was already a GINA replacement before installing AccessAgent), and the Lock screen will show enGINA's Lock screen.

- ❸ On the RDP client, specify the auto-logon credentials in the RDP client.
 1. Click **Options>>**.
 2. Select the **General** tab, then type the credentials.
 3. Mark **Save my password**.

- ❸ After this is done, write a script or batch file, for example `mstsc /v [server-name] /f` to auto launch the RDP client in full screen mode and log on to the remote server, or you can schedule it as an auto-start task after the Thin Client is starting up.



If you are using a different RDP client, you find a similar way to configure it.

Configuring auto-logon for ICA clients

Verify that the following configurations are done on the Citrix server:

In Winlogon registry hive, `GinaDLL=enGINA.dll`.

- ❶ In Encentuate DO registry hive, `TSEnginaLogonNoLocalSessionEnabled=0`
- ❷ In Encentuate registry hive, `PrevGINA=ctxgina.dll`. This is to make sure the EnGINA is chained correctly to Citrix GINA, so that the auto-logon credentials specified in the ICA client can be passed on.

With these three registries set, the Welcome screen shows Citrix Welcome screen, and the Lock screen will show EnGINA's Lock screen.

- ❸ In the ICA client, specify the auto-logon credentials in the ICA client similar to what you do with the RDP client. You can also set the ICA client Window size to be **Full Screen**.
- ❹ Write a simple script/batch file or schedule it as an auto-start task to automatically launch the ICA client in full screen mode and log on to the Citrix server.

Configuring MAC Settings at IMS Server

To configure MAC setting parameters in IMS:

- 1 Run the **IMS Configuration Utility**. Go to **Start >> All Programs >> IMS Server >> IMS Configuration Utility**.
- 2 Under **Basic Settings**, select **ActiveCode Deployment** to open the panel.

ActiveCode deployment

General

Maximum number of ActiveCode verification attempts:
This must be an integer (Minimum:0)

ActiveCode account reset-lockout time, in seconds:
This must be an integer (Minimum:-1)

Mobile ActiveCode validity period, in seconds:
This must be an integer (Minimum:0)

Allowed ActiveCode client IPs:

Enable SSL for ActiveCode client:

ActiveCode access password:

OTP look-ahead number:
This must be an integer (Minimum:1)

OTP no-synchronization window:
This must be an integer (Minimum:1)

OTP token reset window:
This must be an integer (Minimum:1)

Active Code Deployment panel (1/3)

IP-application name bindings:

NASID-application name bindings:
 examplehost,exampleApp

Application binding for MAC/OTP accounts:

Use MAC-only registration of users:

Allow Mobile ActiveCodes to be application-specific:

ActiveDirectory attribute to be displayed for MAC-only registration of users:

Send out Mobile ActiveCodes in upper case:

Search filter used for MAC-only registration of users UI:

Default messaging connector:

Authentication mechanisms for Stage 1:
 ENC_PWD_OR_APP_PWD
 MAC
 AA_OTP
 BYPASS

ActiveCode Deployment panel (2/3)

- 3 Enter the mapping between the RADIUS client name and the MAC-enabled authentication service in the **NASID-application name binding** field.

The entry format should be: "RADIUS client name,authentication service ID".

For example (see [Configuring the RADIUS Interface at IMS Server](#)): If the RADIUS client name is **AventailVPN** and the authentication service ID is **MAC**, this entry should have the value "AventailVPN,MAC".

- 4 Click **Add**.
- 5 Select **true** or **false** from the **MAC-only registration of users** dropdown list to specify whether MAC-only user-registration is supported.



Set the value to "true" to not have users perform self-service sign-up through Web Workplace or AccessAgent.

- 6 Select **true** or **false** from the **Should Mobile ActiveCodes be sent out in upper-case?** dropdown list to determine whether MACs are sent out in uppercase or lowercase.
- 7 Enter a search filter (name value pair in a comma-separated list) in the **Search filter used for MAC-only registration of users user interface** field.

This parameter specifies the comma-separated search filter used when users are searched on the User registration page. For example, `sAMAccountName=*,objectClass=user`.

- 8 Specify the **Default messaging connector**. (see [Configuring a message connector](#) for details).

Authentication mechanisms for Stage 2:

Remove

MAC

Remove

VASCO

Remove

OATH

Remove

BYPASS

Add

Enterprise Directory attributes to be matched before MAC/OTP request/verification:

Values of the Enterprise Directory attribute to be matched before MAC/OTP request/verification:

Add

ActiveCode-enabled authentication services:

Add

Update

Reset

Read-only keys:

Character set, ActiveCode length, algorithm binding

YZ23456789ABCDEFGHIJKLMNPQRSTUVWXYZ,6,AES

WXYZ23456789ABCDEFGHIJKLMNPQRSTUVWXYZ,8,AES

1234567890,8,AES

JKLMNOPQRSTUVWXYZYZ23456789ABCDEFGHI,6,MCA

XYZ23456789ABCDEFGHIJKLMNPQRSTUVWXYZ,6,TRIPLEDES

WXYZ23456789ABCDEFGHIJKLMNPQRSTU,8,TRIPLEDES

2345678901,8,TRIPLEDES

ActiveCode Deployment panel (3/3)

- 9 Click **Update**.

Configuring a message connector

Use the IMS Configuration Utility to set up and list the parameters to configure for the message connector used in sending MAC.



The instructions in this appendix are for configuring a Web-based SMS Connector. Other types of message connectors are configured in the same way.

To configure a Web-based SMS Connector:

- ❶ Run the **IMS Configuration Utility** (*Start >> All Programs >> IMS Server >> IMS Configuration Utility*).
- ❷ Under **Advanced Settings**, go to *Message Connectors >> Add Configuration Group*.
- ❸ Select **Web-based SMS Connector** from the drop-down list and click **Configure** to open the **Web-based SMS Connector** panel.
- ❹ Specify a name for the message connector in the **Message Connector Name** field.
- ❺ Enter the identity attribute in the **Address Attribute Name** field. This will be used as the target address for sending messages.

For example, for an SMS message connector, the attribute will probably be "gsmNumber", which specifies the user's phone number.

- ❻ Enter the GSM country code mapping to the corresponding SMS gateway IP address or hostname (e.g., "65,127.0.0.1") in the **GSM code to gateway mappings** field.

This mapping should be used if there are multiple SMS gateways handling different country codes. If there is only one SMS gateway, this setting can be left empty.

- 7 In the **Default SMS gateway** field, enter the SMS gateway IP address or host-name that will be used if the current GSM code does not match any of the GSM code to gateway mappings.

The screenshot shows a web-based configuration interface for an SMS connector. It is divided into two main sections: 'Basic configuration keys' and 'Advanced configuration keys'. The 'Basic' section includes fields for 'Message Connector Name', 'Address Attribute Name', 'GSM code to gateway mappings' (with an 'Add' button), 'Default SMS gateway', 'Phone number field name', 'Message field name', and 'Other field names' (with an 'Add' button). The 'Advanced' section includes a dropdown for 'Fetch the address attribute from Enterprise Directory' (set to 'False'), a text field for 'Enterprise directory address attribute', an integer field for 'HTTP retry count' (set to 3), and an integer field for 'HTTP timeout, in milliseconds' (set to 30000). At the bottom are 'Add' and 'Reset' buttons.

Web-based SMS Connector

▼ **Basic configuration keys**

Message Connector Name

Address Attribute Name

GSM code to gateway mappings:

Default SMS gateway:

Phone number field name:

Message field name:

Other field names:

▼ **Advanced configuration keys**

Fetch the address attribute from Enterprise Directory:

Enterprise directory address attribute:

HTTP retry count:
This must be an integer (Minimum:1)

HTTP timeout, in milliseconds:
This must be an integer (Minimum:1)

Message connectors panel

- 9 Enter the name of the **Phone Number field** on the target web-form (on the SMS gateway) used to send the SMS.
- 10 Enter the name of the **Message field** on the target web-form (on the SMS gateway) used to send the SMS.
- 11 Specify name-value mappings of the fields (e.g., "group,executives") on the target web-form (on the SMS gateway) in the **Other fields**.
- 12 Under the **Advanced Configuration Keys** panel, in the **Fetch the address attribute from Enterprise Directory** field, set whether the address attribute used by this messaging connector should be fetched from the Enterprise Directory or not.

If set to **false**, the address attribute (specified by "Address Attribute Name") is fetched from the IMS database.

If set to **true**, performance will be degraded as each MAC issuance makes a call to the Enterprise Directory.



To support fetching of multi-valued attributes (like "memberOf"), the ADSI connector should be used for configuring the Enterprise Directory (see the Encentuate IAM Administrator Guide for details).

- 13 Enter the name of the attribute to be looked up from the Enterprise Directory (Active Directory or LDAP server) in the **Enterprise directory address attribute** field.



This needs to be set only if **Fetch the address attribute from Enterprise Directory?** is set to **True**.

If this attribute specifies a phone number, it should be of the format "CountryCode-AreaCode-PhoneNumber", for example, "1-650-4136800", "65--64735110".

- 14 Specify the retry count value in the **HTTP retry count** field.
- 15 Specify the timeout value in the **HTTP timeout (milliseconds)** field.
- 16 Click **Add**.

Enabling MAC for Applications and Users

This section covers the following topics:

- [Provisioning a user for MAC](#)
- [Enabling MAC](#)

Provisioning a user for MAC

An Administrator or Helpdesk officer can register users to use MAC in AccessAdmin. Alternatively, users can perform self-service sign-up through Web Workplace. For procedures on how to register users for MAC, see the Encentuate IAM Administrator Guide.

Enabling MAC

MAC can be enabled for two applications:

- SSL VPN, or;
- The Web (in this case, Web Workplace)

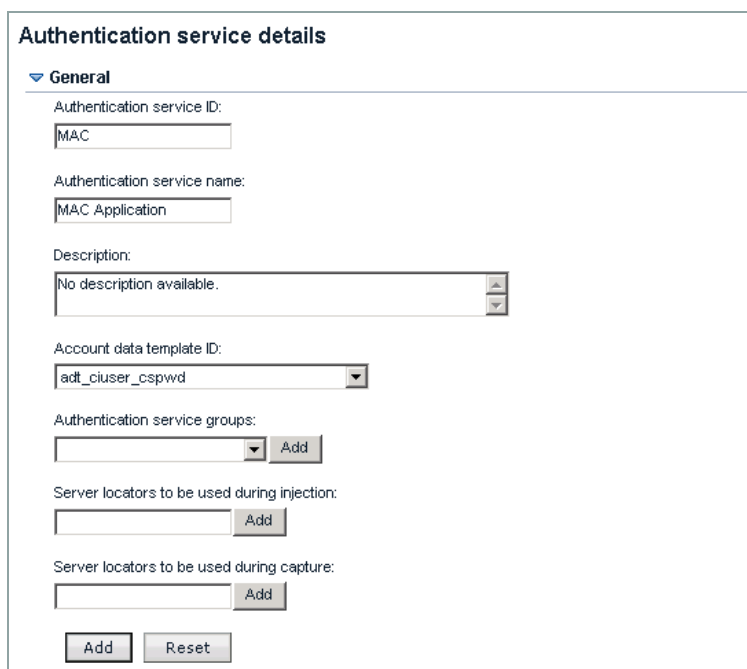
Enabling MAC for SSL VPN

To enable MAC for SSL VPN:

- ❶ Set up using the IMS Configuration Utility.

Add a new authentication service for the MAC-enabled SSL VPN:

1. In the IMS Configuration Utility, add a new Authentication Service by going to: *Basic Settings >> Authentication Services*.
2. Select **AccessAssistant** from the **Authentication Services** drop-down list. Click **Add new service**.



Authentication service details

▼ General

Authentication service ID:

Authentication service name:

Description:

Account data template ID:

Authentication service groups:
 Add

Server locators to be used during injection:
 Add

Server locators to be used during capture:
 Add

Add Reset

Add Authentication Services

3. Enter an **Authentication Service ID**. The ID will appear in the list of Authentication Services already created in IMS Server.
 4. Enter an **Authentication Service Name**. This name is visible to the user.
 5. Click **Add** to save the configuration.
- ② Set up policies for your authentication service using AccessAdmin.

To set policies using AccessAdmin:

1. In the AccessAdmin navigation panel, go to *System >> Authentication Service Policies*.
2. Click the appropriate authentication service in order to change the authentication mode.
3. Under **Authentication Policies**, select the authentication mode(s) to be supported for the authentication service. In this case, **OTP**, **MAC** or both.

Authentication service policies

MAC Application

[Back to Authentication services](#)

► Password Policies

▼ Authentication Policies

Default automatic sign-on password entry option for the authentication service

Enable automatic sign-on?

Authentication modes to be supported

- OTP (Encentuate)
- Password
- SCR
- OTP (OATH)
- OTP (time-based)
- MAC
- CCOW
- CAPi

Prompt user on auto-capture of password?

Maximum number of accounts allowed for the authentication service

Authentication Services Policies panel

4. Click **Update**.

To modify ActiveCode system policies using AccessAdmin:

1. Click **System Policies** in the AccessAdmin navigation panel.
2. Click **ActiveCode Policies**. The ActiveCode Policies panel is expanded.

▼ ActiveCode Policies

Maximum number of Mobile ActiveCodes that may be valid for a user at any time
(Minimum:1, Maximum:7)

ActiveCode bypass option

- Authorization code and enterprise account password
- Authorization code and Encentuate password
- Authorization code and secret

Option for appending a secret to Mobile ActiveCode

Option for appending a secret to OTP (time-based) and OTP (OATH)

Identity attribute name of the Administrator-assigned secret

Number of consecutive OTPs needed for resetting an OTP (OATH) token
(Minimum:1, Maximum:5)

ActiveCode Policies panel

3. Specify the **Maximum number of Mobile ActiveCodes that may be valid for a user at any time**. For example, If a user should only be allowed to use the very last MAC that was issued to him, this policy should be set to 1.
4. Set the **ActiveCode bypass option** to allow users to bypass ActiveCode authentication when they fail to obtain MAC or OTP. Users can also use a combination of authorization code (issued by Helpdesk) and a secret.
5. Set the **Option for appending a secret to Mobile ActiveCode**. If enabled, all MACs entered by users must adhere to the specified format. Note that the order is specified in the policy values.
6. Set the **Option for appending a secret to OTP (time-based) and OTP (OATH)**. If enabled, all OTPs entered by users must adhere to the specified format. Note that the order is also specified in the policy values.
7. Specify the **Identity attribute name of the Administrator-assigned secret** for appending to MAC or OTP.
8. Specify the **Number of consecutive OTPs needed for resetting an OTP (OATH) token**.
9. Click **Update**.

Enabling MAC for a user

Use AccessAdmin to enable MAC for a user. At least one (1) MAC preference should be set, and the appropriate MAC-enabled authentication service must be enabled for the user.

To enable MAC for a user using AccessAdmin:

- ❶ Click the user's name in the AccessAdmin navigation panel.
- ❷ In the **User Profile** panel, enter the MAC phone number and/or e-mail address.

User Profile

Name (first last):

bob doctor

Last name:

doctor

E-mail address:

doctor-bob1@qa.encentuate.com

Encentuate user name:

qa.encentuate.com\doctor-bob1

User principal name:

doctor-bob1@qa.encentuate.com

Mobile ActiveCode phone number:

Country code

Area code

Phone number

Mobile ActiveCode e-mail address:

--NOT FOUND--

Mobile ActiveCode preference 1

--NOT FOUND--

Mobile ActiveCode preference 2

--NOT FOUND--

Mobile ActiveCode preference 3

--NOT FOUND--

Wallet version:

3.x

Update

Reset

AccessAdmin User Profile panel

- 3 Click **Update**.
- 4 Scroll down and expand the **Authentication Policies** panel.

Authentication Policies

Wallet authentication policy

☒ USB Key

☒ Fingerprint

☒ Password

☒ Password + RFID

Enable Mobile ActiveCode authentication?

Yes

Update

AccessAdmin Authentication Policies panel

- 5 Select **Yes** from the **Enable Mobile ActiveCode authentication?** drop-down list.
- 6 Click **Update**.

Configuring the RADIUS Interface at IMS Server

The RADIUS interface at the IMS Server can be configured using the Encentuate IMS Configuration Utility. Follow the steps to configure the RADIUS interface.

This section covers the following topics:

- [Enabling RADIUS](#)
- [Adding a new RADIUS client configuration](#)

Enabling RADIUS

To enable the RADIUS module:

- ❶ In the IMS Configuration Utility, expand the RADIUS Server panel by going to: *Advanced Settings >> User Authentication >> RADIUS Server >> Startup.*
- ❷ From the **Enable RADIUS module** drop-down list, select **yes**.
- ❸ Enter the **RADIUS ServerIP**.
- ❹ Select the **UDP port listening for authentication requests** from the drop-down list. This is the port that the server listens to for RADIUS authentication requests.
- ❺ Select the **UDP port listening for accounting requests** from the drop-down list. This is the port that the server listens to for RADIUS accounting requests.
- ❻ Enter **400** in the **Maximum service queue for the RADIUS server** field. Each authentication request generates one packet, so **400** is a reasonable figure.
- ❼ Select **no** from the **Remove domain component from RADIUS username** drop-down menu. This option strips the domain component from the username.

- 8 Select **yes** from the **Set the Prompt attribute in RADIUS challenge response reply packets** drop-down menu. Some VPNs (notably checkpoint) will not allow RADIUS packets with the **Prompt** attribute set, while others require it to be set.

RADIUS server

Startup

Enable RADIUS module:

RADIUS Server IP:

UDP port listening for authentication requests:

UDP port listening for accounting requests:

Maximum service queue for the RADIUS server:
This must be an integer (Minimum:0)

Remove domain component from RADIUS user name:

Set the Prompt attribute in RADIUS challenge response reply packets:

Allow multiple RADIUS Class attributes:

Enable detailed RADIUS server debug logging:

Clients of this RADIUS server:

Authentication realms for unregistered users:

RADIUS Startup Configuration panel

- 9 Select **no** from the **Allow multiple RADIUS Class attributes** drop-down menu. Enabling this will allow the user's LDAP attributes to be correctly sent as multiple RADIUS Class attributes. However, for VPNs that can handle only one (1) RADIUS Class attribute, this feature must be disabled.
- 10 Select **no** from **Enable detailed RADIUS server debug logging** drop-down menu. Enable this option only for troubleshooting and debugging, since this feature affects performance and privacy.
- 11 In the **Clients of this RADIUS server** field, enter a RADIUS client name, IP address/FQDN, and click **Add**.
- 12 In the **Authentication realms for unregistered users** field, indicate a realm that non-IMS users are authenticated against, then click **Add**. An LDAP type realm can be used to retrieve member of and other user attributes for registered IMS users if the VPN user ID and the LDAP user ID match.
- 13 Click **Update** to save the startup configuration.

Adding a new RADIUS client configuration

You must add a new RADIUS client configuration for every RADIUS client connecting to IMS Server.

To add a RADIUS client configuration:

- 1 Go to *Advanced Settings >> User Authentication >> RADIUS Server >> Add Configuration Group*.
- 2 Select **RADIUS Client** from the drop-down list, then click **Configure**. The RADIUS client panel is displayed.

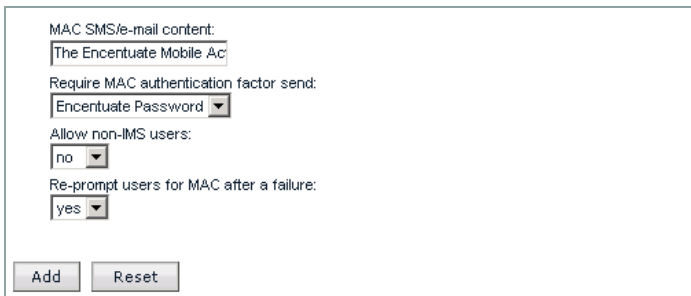
The screenshot shows the 'Radius Client' configuration window. The 'Basic configuration keys' section is expanded, revealing several input fields and a dropdown menu. The fields are: 'Name' (text input), 'Client secret' (text input), 'Vendor-specific attributes' (text input with an 'Add' button), 'Resolvable address of the client' (text input), 'Default unregistered user realm of RADIUS' (text input), 'Enable RADIUS challenge-response' (dropdown menu set to 'yes'), 'Default Challenge message on VPN user interface' (text input with placeholder 'Please enter the Mobile Ac'), 'GSM-SMS Channel Challenge message on VPN user interface' (text input with placeholder 'Please enter the Mobile Ac'), 'E-mail Channel Challenge message on VPN user interface' (text input with placeholder 'Please enter the Mobile Ac'), 'Retry challenge message on VPN user interface' (text input with placeholder 'The Encentuate Mobile Ac'), and 'MAC SMS/e-mail subject' (text input with placeholder 'Encentuate Mobile Active').

Add Configuration Group (1/2)

- 3 In the **Basic Configuration Keys** panel, enter the **Name** of the new client.
- 4 Enter a **Client secret**. This is the shared secret used to encrypt communication between the RADIUS server and client.
- 5 Enter the **Resolvable address of the client**. This is the IP address or FQDN of the host listed as a RADIUS client.
- 6 Select **yes** for **Enable RADIUS challenge-response** to enable RADIUS challenge-response.

- 7 If MAC is enabled, enter the **Default Challenge message on VPN user interface**. This is the default RADIUS challenge message that the user sees on the VPN user interface.
- 8 If MAC is enabled, enter the **GSM-SMS Channel Challenge message on VPN user interface**. This is the RADIUS challenge message that the user sees on the VPN user interface if the MAC is sent using an SMS gateway (e.g., via a Web-based SMS message connector).
- 9 If MAC is enabled, enter the **Email Channel Challenge message on VPN user interface**. This is the RADIUS challenge message that the user sees on the VPN user interface if the MAC is sent using an email gateway (such as, via an Email message connector).
- 10 Enter the **Retry challenge message on VPN user interface**. This is the RADIUS challenge message that the user sees on the VPN user interface when asked to retry following a failed verification attempt.
- 11 Enter the **Subject of MAC SMS or e-mail**. This is the template for the subject of the SMS or email message that will contain the MAC to be sent to the user. Use the placeholder "%MAC%" to indicate where the MAC should appear.

For example, if the text is "Your MAC is %MAC%", and the MAC is "5yd34t", the actual subject of the message will be "Your MAC is 5yd34t".



MAC SMS/e-mail content:
The Encentuate Mobile Ac

Require MAC authentication factor send:
Encentuate Password

Allow non-IMS users:
no

Re-prompt users for MAC after a failure:
yes

Add Reset

Add Configuration Group (2/2)

- 12 Enter the **Body of MAC SMS or e-mail**. This is the template for the body of the SMS or email message will contain the MAC to be sent to the user. Use the placeholder "%MAC%" to indicate where the MAC should appear.

For example, If the text is "Your MAC is %MAC%", and the MAC is "5yd34t", the actual body of the message will be "Your MAC is 5yd34t".

- 13 Select **yes** to **Allow users for MAC after a failure** if it is entered incorrectly. The user will be prompted until the account is locked.
- 14 Click **Add**. The *Startup Configuration >> Configured Keys* panel is displayed.
- 15 Restart the IMS Server for the changes to take effect.

Integrating with Aventail SSL VPN

Aventail SSL VPN is one of the various VPN appliances supported by the IAM Remote Access Integration.

Configure the Aventail SSL VPN appliance to use the IMS Server as an authentication server, and launch applications from Web Workplace.

This section covers the following topics:

- [Configuring the VPN Server](#)
- [Configuring authentication servers](#)
- [Configuring realms](#)
- [Configuring services](#)
- [Configuring resources](#)
- [Configuring Aventail WorkPlace](#)
- [Configuring Access Control](#)
- [Configuring SSL settings](#)
- [Completing the configuration](#)

Configuring the VPN Server

Configure the VPN server to store the shared secret used for authentication. The following information needs to be stored:

- Name of server: This should be a DNS-resolvable name or IP address
- Shared secret
- Authorization port (usually 1812)

Configuring authentication servers

To configure authentication servers:

- 1 Log on to the Management Console of Avenail SSL VPN .
- 2 From the main navigation menu, click **Authentication Servers**. The **Authentication Servers** page is displayed.
- 3 Click **New...** to define a new authentication server.
- 4 Select **RADIUS** as the authentication directory type, and click **Continue**.
- 5 Enter a name for the authentication server.
- 6 Enter the host name or IP address of the IMS Server as that of the **primary RADIUS server**. If the IMS Server is configured to listen on something other than 1645 (the known standard), you can specify a port number as a colon-delimited suffix, for example, ims.company.com:1812.
- 7 Enter the RADIUS client secret that you have specified in the IMS Server RADIUS configuration as the **shared secret** here.
- 8 Click **Save** to store the configuration.

Configuring realms

To configure realms:

- 1 From the main navigation menu, click **Realms**. The Realms page is displayed.
- 2 Click **New** to define a new realm.
- 3 Enter a name for the realm and select the IMS authentication server you have defined above as the authentication server.
- 4 Click **Finish** to store the configuration.

Configuring services

To configure services:

- 1 From the main navigation menu, click **Services**. The Services page is displayed.
- 2 In the **Access services** area, click the **Configure** link for **Web proxy service**. The Configure Web Proxy Service page is displayed.

- ③ Click the **Web Application Profiles** tab, and then click **New**. The Add/Edit Web Application Profile page is displayed.
- ④ Enter an appropriate name to the Web Workplace profile (e.g., "WWPAuth").
- ⑤ Under the **Single Sign-On** section, choose **Forward each user's individual user-name and password**.
- ⑥ Under the **Content translation** section, choose the following options: **Translate cookie body** and **Translate cookie path**.

Configuring resources

To configure resources:

- ① From the main navigation menu, click **Resources**. The Resources page is displayed.
- ② Under the *Resources* tab, click **New** and select **URL....**
- ③ Give an appropriate name to the resource (e.g., "WWP").
- ④ Give the **URL** of the Web Workplace hosting server (e.g., <https://ims.com-pany.com>).
- ⑤ Mark the **Create shortcut on WorkPlace** checkbox so that steps 1 to 4 in the **Configure WorkPlace** section below can be simplified.
- ⑥ Under the **Advanced Web resource options** section, give the resource an **Alias name** (e.g., "wwp") and choose the **web application profile** created earlier (e.g., "WWPAuth").
- ⑦ Click **Save** to store the configuration.

Configuring Aventail WorkPlace

To configure Aventail WorkPlace:

- ① From the main navigation menu, click **Aventail WorkPlace**. The Aventail WorkPlace page is displayed.
- ② In the **WorkPlace shortcuts** tab, click **New** and select **Web shortcut....**
- ③ Give an appropriate Number, and Link text.
- ④ Choose the **Resource** configured earlier (e.g., "WWP") and click **Next**.
- ⑤ For the **Start** page, provide the link relative to the URL given above.

- For the Web Workplace portal page, use the URL: "[/WebWorkplacePath/index_basic_auth.jsp](#)", where WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it.
- For each Web application to be embedded in the enterprise portal, use a URL of the form:

["/WebWorkplacePath/link_auto_logon.jsp?&acctClass=authserviceid&app-Name=appid&refresh=true"](#)

where: WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it; authserviceid is the authentication service ID to be used, and appid is the application ID of the application. The following is an example link:

["/WebWorkplace/link_auto_logon.jsp?&acctClass=dir_yahoo&app-Name=app_yahoo_web&refresh=true"](#).

- 6 Click **Finish** to store configuration.
- 7 From the main navigation menu, click **Services**. The Services page is displayed.
- 8 Click the **Configure** link for Aventail WorkPlace in the Access services section. The Configure Workplace page is displayed.
- 9 Under **Web shortcut access**, select the **Use Web content translation (provides single sign-on)**.
- 10 Click **Save** to store configuration.

Configuring Access Control

To configure Access Control:

- 1 From the main navigation menu, click **Access Control**. The Access Control page is displayed.
- 2 Ensure that the access control rules allow your users to access the resources defined above.

Configuring SSL settings

To configure SSL settings:

- 1 From the main navigation menu, click **SSL Settings**. The SSL Settings page is displayed.
- 2 Click the **Edit** link in the **CA certificates** section.

- ③ Click **New** to import the IMS Root CA certificate (and the Web Workplace site certificate, if they are different).
- ④ Choose **Certificate file** to import each certificate. To get the certificate of a Web site using Internet Explorer:
 1. Visit the Web site.
 2. Click **lock** to view certificates.
 3. Click the **Details** tab and **Copy to File...** to export the certificate as a .CER file, which can then be imported into the Aventail SSL VPN .

Completing the configuration

To complete the configuration:

- ① Click **Pending changes** on the top right, and click **Apply Changes**.
- ② On the next user logon to the Aventail SSL VPN , Web Workplace should be visible as a configured application. Aventail SSL VPN can log on to Web Workplace automatically when clicked.

Integrating with Juniper SSL VPN

You must configure the Juniper SSL VPN appliance to use the IMS Server as an authentication server, and to treat Web Workplace as a resource from which applications can be launched.

This section covers the following topics:

- [System requirements](#)
- [Configuring authentication servers](#)
- [Configuring user realms](#)
- [Configuring signing-in](#)
- [Configuring Web resources profiles](#)
- [Configuring terminal services resources](#)
- [Configuring SSL settings](#)
- [Embedding application links](#)

System requirements

Supported software versions

- Juniper Networks Secure Access (SA) series of SSL VPN appliances, firmware version 5.4 and above
- Encentuate IMS Server 3.3.0.0 and above
- Encentuate Web Workplace 3.3.0.4 and above

- Encentuate AccessAgent 3.3.0.2 and above

Supported Web browsers

Any standard Web browser that supports JavaScript and cookies. The default configuration of these Web browsers are supported:

- Microsoft Internet Explorer 6.0 SP1 and above on Windows
- Mozilla Firefox 1.5 and above on Windows and Linux

To enable the use of Juniper's Terminal Services Clients for accessing Windows Terminal Services or Citrix, install and enable any of the following:

- ActiveX
- Microsoft JVM
- Sun JVM 1.5.0 plug-in

Supported second factors

- Any SMS or paging client:
 - Mobile phone
 - Smartphone
 - PDA
 - Pager
- Any email client:
 - Mobile phone
 - Smartphone
 - PDA
 - Web-based email system
- OTP tokens:
 - Authenex A-Key OATH-only token (OATH-based OTP)
 - VASCO Digipass GO 3 (time-based OTP)

Network requirements

Only the following TCP ports are allowed through the enterprise firewall to the Juniper SSL VPN appliance:

- 80 (HTTP)
- 443 (HTTPS)

Configuring authentication servers

To configure authentication servers:

- ❶ Log on to the **Central Manager** of the Juniper SSL VPN.
- ❷ Click **Auth. Servers** from the main navigation menu. The Authentication Servers page is displayed.
- ❸ Go to (Select server type) >> *Radius Server* >> *New Server...* to define a new authentication server.
- ❹ Enter a name for the authentication server.
- ❺ Enter the host name or IP address of the IMS Server as that of the RADIUS Server. If the IMS Server is configured to listen on something other than 1645 (the standard), you can specify a port number in Authentication Port.
- ❻ Enter the RADIUS client secret that you have specified in the IMS Server RADIUS configuration as the Shared Secret here.
- ❼ Enter the IP address of the Juniper SSL VPN in **NAS-IP-Address** field.
- ❽ Mark the **Users authenticate using tokens or one-time passwords** checkbox.
- ❾ Under **Custom challenge expressions**, mark the **Generic Login** checkbox and enter (.*) in the corresponding text box.
- ❿ Click **Save Changes** to store the configuration.

Configuring user realms

To configure user realms:

- ❶ Click **User Realms** from the main navigation menu. The User Authentication Realms page is displayed.
- ❷ Click **New** to define a new realm.
- ❸ Enter a name for the realm and select the IMS authentication server you have defined above as the authentication server.
- ❹ Click **Save Changes** to store the configuration.

Configuring signing-in

To configure signing-in:

- ❶ Click **Signing In** from the main navigation menu. The **Signing In** page is displayed.
- ❷ Select the **Sign-in Pages** tab, and click the **Upload Custom Pages...** button.
- ❸ Click **Sample** to download a ZIP file containing sample sign-in pages from the **Sample Template Files** panel.
- ❹ Modify both **Defender.html** and **Defender-ppc.html** in the ZIP file as follows:
 1. Delete the word: "Challenge: "
 2. Delete the line: "<p class='cssSmall'>Enter the challenge string above into your token, and then enter the one-time response in the field below.</p>"
 3. Replace the word "Response:" with "Mobile ActiveCode:".
- ❺ Rename the ZIP file as **sign-in_mac.zip**.
- ❻ Enter **Mobile ActiveCode Sign-In Page** as Name for the custom sign-in pages.
- ❼ Click **Browse...** and select the ZIP file **sign-in_mac.zip**.
- ❽ Click **Upload Custom Pages** to upload the custom sign-in pages.
- ❾ Select the **Sign-in Policies** tab.
- ❿ Under **User URLs**, click ***/** to configure user sign-in to use the newly-created custom sign-in pages.

- 11 Select **Mobile ActiveCode Sign-In Page** for **Sign-in page**.
- 12 Make sure that **IMS** is in the list of **Selected realms** under the **Authentication realm**.
- 13 Click **Save Changes** to store the configuration.

Configuring Web resources profiles

To configure Web resource profiles:

- 1 Click **Resource Profiles** from the main navigation menu. The **Resource Profiles** page is displayed.
- 2 Click **Web Applications/Pages >> New Profile...** to create a new Web resource.
- 3 Give an appropriate name to the resource (e.g., **Web Workplace**).
- 4 Give the Base URL of the Web Workplace hosting server (e.g., **https://ims.company.com**).
- 5 Click **Show ALL autopolicy types >>** to configure advanced policies.
- 6 Mark **Autopolicy: Single Sign-on** and click **Basic Auth**.
- 7 Click the **Use predefined credentials...** and **Variable Password:** radio buttons. Enter "<USER>" for Username and "<PASSWORD>" in the **Variable Password** field.
- 8 Click **Save and Continue >** to store the configuration.
- 9 Select appropriate Roles and click **Save Changes**.
- 10 Select the **Bookmarks** tab and click the automatically created bookmark.
- 11 Enter **"/WebWorkplace/index_basic_auth.jsp"** in the URL field.
- 12 Click **Save Changes** to store the bookmark. This will be the bookmark for accessing Web Workplace.
- 13 Click **New Bookmark...** to create a bookmark for accessing a Web application through Web Workplace.
- 14 Enter a name for the Web application.
- 15 Use the following URL format:

["/WebWorkplacePath/link_auto_logon.jsp?&acctClass=authserviceid&app-Name=appid&refresh=true"](#)

where: WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it; authserviceid is the authentication service ID to be used, and appid is the application ID of the application. The following is an example link:

["/WebWorkplace/link_auto_logon.jsp?&acctClass=dir_yahoo&app-Name=app_yahoo_web&refresh=true"](/WebWorkplace/link_auto_logon.jsp?&acctClass=dir_yahoo&app-Name=app_yahoo_web&refresh=true).

- 16 Click **Save Changes** to store the bookmark.

Configuring terminal services resources

To configure terminal services resources:

- 1 Click **Resource Profiles** from the main navigation menu. The **Resource Profiles** page is displayed.
- 2 Click **Terminal Services** and then **New Profile...** to create a new Terminal Services resource.
- 3 Give an appropriate name to the resource (e.g., "Terminal Server").
- 4 Enter the host name or IP address of the terminal server as Host.
- 5 Click **Save and Continue >** to store the configuration.
- 6 Select appropriate **Roles** and click **Save Changes**.
- 7 Select the **Bookmarks** tab and click the automatically created bookmark.
- 8 Under **Authentication**, enter "<USER>" for Username and "<PASSWORD>" for **Variable Password**.
- 9 Click **Save Changes** to store the bookmark. This will be the bookmark for accessing terminal services.

Configuring SSL settings

To configure SSL settings:

- ❶ Click **Configuration** from the main navigation menu. The Configuration page is displayed.
- ❷ Select the **Certificates** tab.
- ❸ Click **Trusted Server CAs**.
- ❹ Click **Import Trusted Server CA...** to import the IMS Root CA certificate (and the Web Workplace site certificate, if they are different).
- ❺ Click **Browse...** to import the certificate. Visit the Web site, and click the **lock** icon to view certificates and get the certificate of a Web site using Internet Explorer. Select the **Details** tab and click **Copy to File...** to export the certificate as a .CER file, which can then be imported into the SSL VPN.
- ❻ Click **Import Certificate** to complete the process.

Embedding application links

Enterprise portal

Links to Web applications, Windows Terminal Servers, and Citrix servers, can be embedded in an enterprise portal. The following are instructions for embedding such links:

Web application

For each Web application to be embedded in the enterprise portal, use a URL of the form:

[https://WebWorkplaceHost/WebWorkplacePath/
link_auto_logon.jsp?&acctClass=authserviceid&appName=appid&refresh=true](https://WebWorkplaceHost/WebWorkplacePath/link_auto_logon.jsp?&acctClass=authserviceid&appName=appid&refresh=true)

where: WebWorkplaceHost is the hostname of the Web server hosting Web Workplace; WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it; authserviceid is the authentication service ID to be used, and appid is the application ID of the application.

The following is an example link:

[https://ims.company.com/WebWorkplace/
link_auto_logon.jsp?&acctClass=dir_yahoo&appName=app_yahoo_web&refresh=true](https://ims.company.com/WebWorkplace/link_auto_logon.jsp?&acctClass=dir_yahoo&appName=app_yahoo_web&refresh=true)

Windows Terminal Server or Citrix server

Refer to the Juniper Networks Secure Access Administration Guide for instructions on creating links from an external site to a terminal services session bookmark.

The following is an example link:

<https://<IVE>/dana/term/winlaunchterm.cgi?bmname=<bookmarkName>>

Web Workplace portal page

To embed the Web Workplace portal page in the enterprise portal, use a URL of the form:

https://WebWorkplaceHost/WebWorkplacePath/index_basic_auth.jsp

where: WebWorkplaceHost is the hostname of the Web server hosting Web Workplace; and WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it.

The following is an example link:

https://ims.company.com/WebWorkplace/index_basic_auth.jsp

Integrating with F5 SSL VPN

You need to configure the F5 SSL VPN appliance to use the IMS Server as a RADIUS authentication server for a user group, and to treat Web Workplace as a Web application resource.

This section covers the following topics:

- [System requirements](#)
- [Configuring user group](#)
- [Customize WebDAV](#)
- [Configuring Web application resources](#)
- [Configuring terminal server resources](#)
- [Embedding application links in an enterprise portal](#)

System requirements

Supported software versions

- F5 Networks FirePass series of SSL VPN appliances, firmware version 6.0 and above
- Encentuate IMS Server: 3.3.0.0 and above
- Encentuate Web Workplace: 3.3.0.4 and above
- Encentuate AccessAgent: 3.3.0.2 and above

Supported Web browsers

Any standard Web browser that supports JavaScript and cookies. The default configuration of these Web browsers are supported:

- Microsoft Internet Explorer 6.0 SP1 and above on Windows
- Mozilla Firefox 1.5 and above on Windows and Linux

To enable the use of F5 Terminal Services Clients for accessing Windows Terminal Services or Citrix, install and enable any of the following:

- ActiveX
- Sun JVM

Supported second factors

- Any SMS or paging client:
 - Mobile phone
 - Smartphone
 - PDA
 - Pager
- Any email client:
 - Mobile phone
 - Smartphone
 - PDA
 - Web-based email system
- OTP tokens:
 - Authenex A-Key OATH-only token (OATH-based OTP)
 - VASCO Digipass GO 3 (time-based OTP)

Network requirements

Only the following TCP ports are allowed through the enterprise firewall to the Juniper SSL VPN appliance:

- 80 (HTTP)
- 443 (HTTPS)

Configuring user group

To configure user group:

- ❶ Log on to the Admin Console of the F5 SSL VPN.
- ❷ In the navigation pane, click **Users**, expand **Groups**, and click **Master Groups**. The Master Groups screen is displayed.
- ❸ Click the **Create new group** button.
- ❹ Enter a name for the group (e.g., "IMS").
- ❺ Select **External** for users in group
- ❻ Select **RADIUS** for authentication method.
- ❼ Click **Create** to create the new group.
- ❽ Select the **Authentication** tab.
- ❾ Enter the host name or IP address of the IMS Server in the **Server** field. If the IMS Server is configured to listen on something other than 1645 (the standard), you can specify a port number in Port.
- ❿ Enter the RADIUS client secret that you have specified in the IMS Server RADIUS configuration as the **Shared Secret**. Enter the same thing in **Confirm Shared Secret**.
- ⓫ Click **Save Settings** to store the configuration.
- ⓬ Select the **Resource Groups** tab.
- ⓭ Click an available resource group (e.g., Default_resource) and click the **Add >** button to assign resources.
- ⓮ Click **Update** to store the configuration.

- 15 Click **Global Settings** in the navigation pane. The Global Settings screen is displayed.
- 16 Mark the **Use extra domain password for single sign on** checkbox and click **Update** to store the configuration.

Customize WebDAV

The FirePass user logon page should be customized to hide the extra domain password field, since it is supposed to be the same as the user's Encentuate password.

To customize WebDAV:

- 1 Create an **HTTP Web Service** on the Device Management : Configuration : Network Configuration : Web Services screen to enable WebDAV-based customization.
- 2 Select the **Allow insecure access** option on the Device Management : Security : User Access Security screen.
- 3 Mark the **Allow WebDAV sandbox customization** checkbox on the Device Management : Customization screen and enter a WebDAV password in the text box that is displayed.
- 4 The WebDAV sandbox is accessed via HTTP at the URI **/sandbox** as the user **webdav**. For example, if the FirePass controller has been configured using the steps above with an HTTP web service at 192.168.0.99, use the URL <http://192.168.0.99/sandbox/>.
- 5 Go to the FirePass user logon page and save it as **index.htm**.
- 6 Modify **index.htm** as follows:

1. Delete the domain password label and input field:

```
<tr valign=top>
```

```
<td></td>
```

```
<td align=left><span class=o>Domain password<br>(use cached if
empty) :</span><br></td>
```

```
</tr>
```

```
<tr valign=top>
```

```
<td></td>
```

```
<td align=left><input type=password class=lp_input size="13"
name="dpassword" autocomplete="off"><br></td>

</tr>
```

2. Insert this script right after the deleted domain password label and input field:

```
<INPUT type="hidden" name="dpassword">

<SCRIPT LANGUAGE='VBScript'>

sub Setdpassword()

    e1.dpassword.Value = e1.password.Value

end sub

</SCRIPT>
```

3. Change the **onclick** property of the logon button by replacing the line:

```
<input name=login id=submitform type=submit class=o
value="Logon">

with:

<input name=login id=submitform onclick='Setdpassword()' '
type=submit class=o value="Logon">
```

7 Upload **index.htm** to FirePass using WebDAV.

1. Launch **My Network Places** in Windows.
2. Click **Add a network place**.
3. Click **Next** twice.
4. Enter the URL stated in step 4 above,
5. Log on using webdav as the user name and the WebDAV password as the password.
6. Drag and drop the **index.htm** file into the explorer window.

Configuring Web application resources

To configure Web application resources:

- ❶ Click **Portal Access** in the navigation pane. Expand **Web Applications** and click **Resources**. The **Resources** screen is displayed.
- ❷ Click **Add New Favorite** to create a favorite for accessing a Web application through Web Workplace.
- ❸ Enter a name for the Web application.
- ❹ Use a URL of the form:

["https://WebWorkplaceServer/WebWorkplacePath/link_auto_logon.jsp?&acctClass=authserviceid&appName=appid&refresh=true"](https://WebWorkplaceServer/WebWorkplacePath/link_auto_logon.jsp?&acctClass=authserviceid&appName=appid&refresh=true)

where: WebWorkplaceServer is the server hosting Web Workplace; WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it; authserviceid is the authentication service ID to be used, and appid is the application ID of the application. The following is an example link:

["https://www.encentuate.com/WebWorkplace/link_auto_logon.jsp?&acctClass=dir_yahoo&appName=app_yahoo_web&refresh=true"](https://www.encentuate.com/WebWorkplace/link_auto_logon.jsp?&acctClass=dir_yahoo&appName=app_yahoo_web&refresh=true).

- ❺ Mark the **Open in new window** checkbox.
- ❻ Click **Add New** to store the favorite.
- ❼ Include the appropriate URLs in the **Allow list** under **Access Control Lists**.
- ❽ Click **Master Group Settings** in the navigation pane. The Master Group Settings screen is displayed.
- ❾ Select the **Master Group** that you created earlier (e.g., IMS).
- ❿ Under **NTLM and Basic Auth Proxy**, mark the checkboxes for **Proxy Basic and NTLM auth using FirePass user logon form**, and **Auto-logon to Basic and NTLM auth protected sites using FirePass user credentials**. Then select **Basic Authentication** as the Preference.

Configuring terminal server resources

To configure terminal server resources:

- ❶ Click **Application Access** in the navigation pane. Expand **Terminal Servers**, and click **Resources**. The Resources screen is displayed.
- ❷ Click **Add New Favorite** to create a favorite for accessing a Terminal Server.
- ❸ Enter a name for the Terminal Server.
- ❹ Enter the host name or IP address of the Terminal Server in the **Host** field.
- ❺ Select **Microsoft Terminal Server** for Port.
- ❻ Click **Add New** to store the favorite.
- ❼ Click **Master Group Settings** in the navigation pane. The Master Group Settings screen is displayed.
- ❽ Select the **Master Group** that you created earlier (e.g., IMS).
- ❾ Mark the **Auto-logout to applicable Terminal Servers using FirePass user login credentials** checkbox under **Screen resolution**.

Embedding application links in an enterprise portal

Links to Web applications, Windows Terminal Servers, and Citrix servers, can be embedded in an enterprise portal. The following are instructions for embedding such links:

Web application

For each Web application to be embedded in the enterprise portal, use a URL of the form:

["https://WebWorkplaceHost/WebWorkplacePath/link_auto_logon.jsp?&acctClass=authserviceid&appName=appid&refresh=true"](https://WebWorkplaceHost/WebWorkplacePath/link_auto_logon.jsp?&acctClass=authserviceid&appName=appid&refresh=true)

where: WebWorkplaceHost is the hostname of the Web server hosting Web Workplace; WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it; authserviceid is the authentication service ID to be used, and appid is the application ID of the application.

The following is a sample link:

https://ims.company.com/WebWorkplace/link_auto_logon.jsp?&acctClass=dir_yahoo&appName=app_yahoo_web&refresh=true

Windows Terminal Server or Citrix server

To obtain a direct link to the FirePass Terminal Server client, you can log on to FirePass, launch your Terminal Server favorite, and copy the URL that shows up in the URL field of the browser.

The following is a sample link:

<https://<FirePass>/vdesk/index.php3?Z=0,7>

Web Workplace portal page

To embed the Web Workplace portal page in the enterprise portal, use a URL of the form:

https://WebWorkplaceHost/WebWorkplacePath/index_basic_auth.jsp

where: WebWorkplaceHost is the hostname of the Web server hosting Web Workplace; and WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it.

The following is an example link:

https://ims.company.com/WebWorkplace/index_basic_auth.jsp

Integrating an Application with MAC Using SOAP API

This section covers the following topics:

- [Basic concepts](#)
- [Required components](#)
- [Logging on with an MAC](#)
- [Using API](#)
- [API Data](#)
- [API operations](#)
- [Enabling MAC authentication for an application using the SOAP API](#)
- [WDSL](#)

Basic concepts

Encentuate Mobile ActiveCode service module

The Encentuate Mobile ActiveCode Service Module is an IMS Service module that generates and verifies single-use, random, event-based authentication codes (ActiveCodes) for strong authentication.

Simple Object Access Protocol (SOAP)

SOAP is a protocol for exchanging XML-based messages over a computer network, normally using HTTP. SOAP forms the foundation layer of the Web services stack, providing a basic messaging framework that more abstract layers can build on.

SOAP services are defined using WSDL (Web Services Definition Language) and are accessible through a URL known as a SOAP endpoint.

Encentuate IAM provides a SOAP API for applications to communicate with the IMS Server to perform MAC authentication. With the SOAP API, the request interface is an object in your application's native programming language.

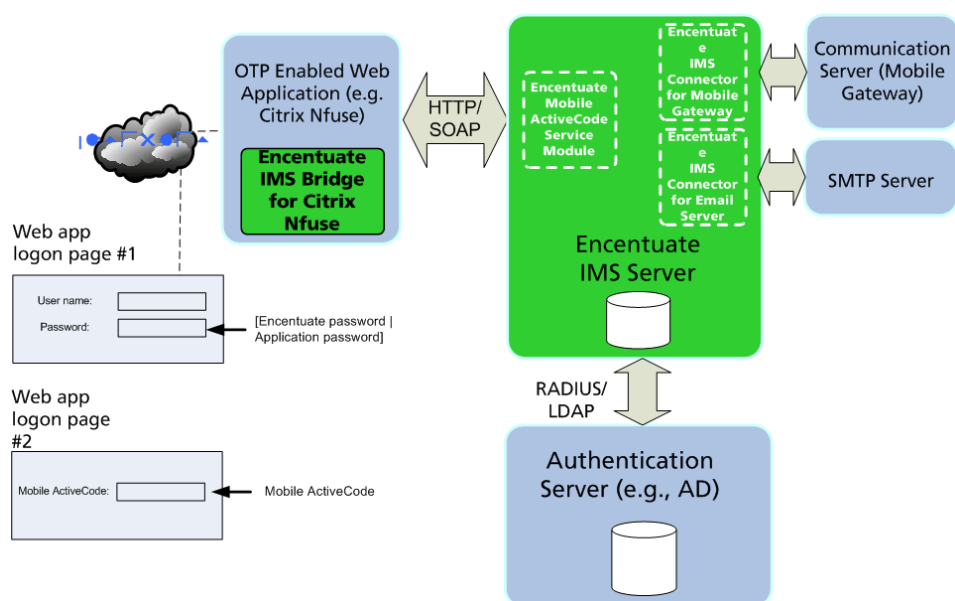
A third-party SOAP client can be used to generate business-object interfaces and network stubs from a WSDL document that specifies the IMS Server message schema, the service address, and other information. The SOAP client handles the details of building the SOAP request and sending it to the IMS Server, while your application works with data in the form of object properties, as it sends and receives data by calling object methods.

Required components

The components required are:

- IMS Server
- Mobile ActiveCode Service Module
- At least one of the following: Mobile Gateway, Communication Server, and/or Email Server
- IMS Connector for Mobile Gateway, Communication Server, or Email Server

Logging on with an MAC



Architecture Overview of Mobile ActiveCode
(customized application logon interface using SOAP for MAC verification)

To log on to an application:

- 1 Launch the application logon interface.
- 2 Enter your Encentuate user name and password.

The logon interface requests for an MAC, which is re-directed to the IMS Server using SOAP.



You may need to enter your application user name and password at the logon interface. This allows applications to use MAC authentication without requiring signup with Encentuate IAM. However, you must be registered by an Administrator through AccessAdmin.

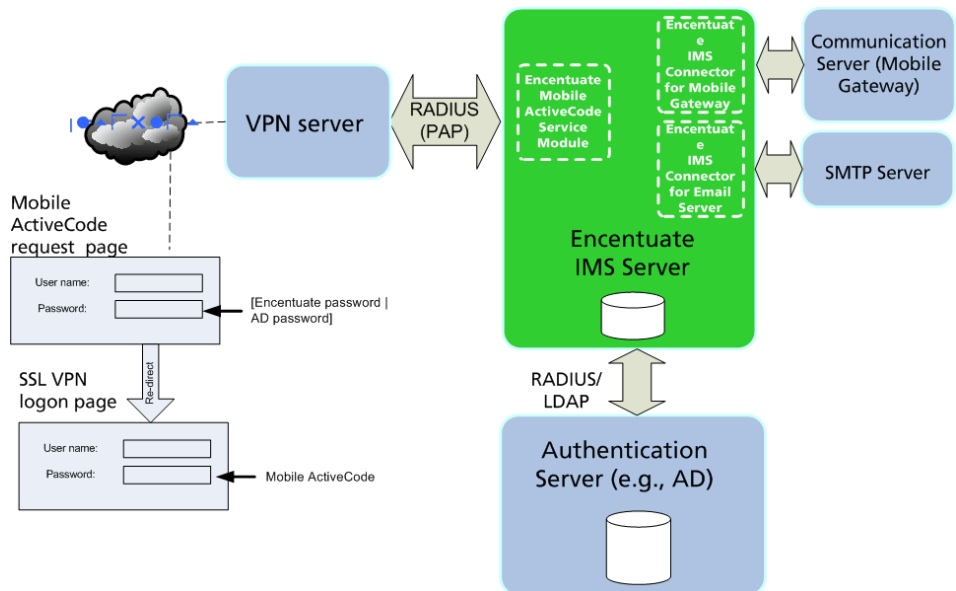
- 3 Choose a preferred channel (e.g., email or mobile phone) from the logon interface for the MAC to be sent.

The IMS Server then delivers an MAC to the user's pre-registered email address or mobile phone.

- 4 After receiving the MAC, enter the MAC on the application logon interface.

The application verifies the MAC with the IMS Server using SOAP again.

If the application logon interface cannot be customized to request for an MAC (e.g., a Windows application), a separate request MAC Web page may be needed.



Architecture Overview of Mobile ActiveCode
(non-customizable application logon interface using RADIUS for MAC verification)

To make a separate MAC Web page request:

- ❶ Launching the request MAC Web page.
- ❷ Enter your Encentuate user name and password.
- ❸ Choose a preferred channel for the MAC to be sent.

The request MAC Web page requests for an MAC, which is re-directed to the IMS Server using SOAP. The IMS Server then delivers an MAC to the user's email address or mobile phone.

- ❹ After receiving the MAC, launch the application and enter the MAC on the application logon interface.

The application verifies the MAC with the IMS Server via RADIUS.

Using API

To use the API on a typical setup:

- ❶ Call requestOtp (if user submits application password) or requestOtpWithPasscode (if user submits Encentuate password) to request for MAC to be sent to the user.
- ❷ Call verifyOtp to verify that a submitted MAC is valid. If so, allow user to log on to the application, or the system displays a prompt that MAC is invalid.

If the application caches the MAC and verifies the user's submitted MAC directly, step 2 may be omitted.

API Data

This section specifies the data types and values that are used by this API.

resultCode

```
<element name="resultCode" type="xsd:int" />
```

Synopsis

The result code that is returned by an operation to indicate the operation's success or the reason for failure.

Value

Identifier	Value (Hex)	Description
OTP_SUCCESS	0x03007200	MAC request/verification is successful.
OTP_ILLEGAL_OTP	0x53007201	MAC is invalid.
OTP_ILLEGAL_PASSCODE	0x53007202	Encentuate password is incorrect.
OTP_ILLEGAL_CLIENT_IP	0x53007203	SOAP client IP address is not allowed.
OTP_ILLEGAL_CLIENT_PASSWORD	0x53007204	clientPassword (shared secret) is incorrect.
OTP_ILLEGAL_LOGINID	0x53007205	loginId (Encentuate user name) is invalid.
OTP_DB_MISSING_ODTPDATA	0x23007209	MAC is not in the database.
OTP_SSL_REQUIRED	0x5300720A	Only SSL access is allowed and SOAP request is not via SSL.
OTP_LOGINID_NOT_FOUND	0x5300720C	loginId (Encentuate user name) is not found in the database.
OTP_DATA_ENCRYPT_FAIL	0x2300720E	Hash algorithm is not supported.
OTP_ACCT_LOCKOUT	0x5300720F	Account is locked out after a maximum number of failed attempts.
OTP_GET_DBTIME_FAIL	0x23007210	Unable to obtain database time.
OTP_LOCKOUT_TIME_NOT_FOUND	0x23007211	Unable to obtain account lock-out time.
OTP_DB_EXCEPTION	0x23007212	Invalid MAC data in the database.
OTP_CHANNELINFO_INVALID	0x23007213	Channel attribute is invalid.
OTP_EXPIRED_OTP	0x23007214	MAC has expired.

Identifier	Value (Hex)	Description
OTP_INVALID_APP_PWD	0x23007215	appPwd (application password) is incorrect.
OTP_APPEND_OTPLIST_FAILED	0x23007217	Error in adding MAC to list of valid MACs.
OTP_APP_INVALID	0x23007218	appld (application ID) is invalid.
OTP_ID_TYPE_VALUE_INVALID	0x23007219	idTypeValue (application type and ID) is invalid.
OTP_INVALID_NAS_ID	0x2300721A	idTypeValue (application type and ID) is invalid.

resultString

```
<element name="resultString" nillable="true" type="xsd:string"
/>
```

Synopsis

The result string that is returned by an operation to indicate the operation's output.

Value

XML snippet of the form:

```
<result>

  <otp>mac</otp>

  <channel>connectorName</channel>

</result>
```

"**mac**" is the MAC that has been generated, if it is to be returned by the operation.

"**connectorName**" is the name of the messaging connector that was used by the operation.

ResultMessage

```
<complexType name="ResultMessage">

  <sequence>

    <element name="resultCode" type="xsd:int" />

  </sequence>

</complexType>
```



```

        <element name="resultString" nillable="true"
type="xsd:string" />

    </sequence>

</complexType>

<element name="ResultMessage" nillable="true"
type="tnsl:ResultMessage" />

```

Synopsis:

The composite result message that is returned by an operation to indicate the operation's success/failure as well as its output.

Value:

resultString is nil if **resultCode** is not **OTP_SUCCESS**.

API operations

This section specifies the operations that are offered by this API.

requestOtp

```

public ResultMessage requestOtp(

    String clientPassword, String idTypeValue, String uid,

    String appPwd, boolean save, String channel, String
msgFormat);

```

Synopsis

Requests for an MAC from the IMS Server using the user's application password.

This operation requests the IMS Server to generate an MAC and send it to the user's phone/pager/email according to the user's preference or the channel specified in the arguments, after verifying the user's application password.

Arguments

clientPassword

Shared secret between the SOAP client and IMS Server. It is configured on the IMS Server using the `auth.otp.access_password` key in **ims.xml**, which can be set using the IMS Configuration Utility.

idTypeValue

Specifies the authentication service as configured in the IMS Server. It can be in either of the following formats (in the example below, **"dir_mac_app"** is the authentication service ID):

- `<appldType>IP</appldType> <appldValue>10.1.16.165</appldValue>`
- `<appldType>nasId</appldType> <appldValue>10.1.16.165</appldValue>`
- `<appldType>appName</appldType> <appldValue>dir_mac_app</appldValue>`

For the first two formats, the IP/nasId should be configured in IMS using the appropriate key in **ims.xml**, which can be set using the IMS Configuration Utility (*ActiveCode Deployment >> IP-Application Name Binding* and *ActiveCode Deployment >> NASID-Application Name Binding*):

```
<auth.otp.ipAppBinding>
    <value xml:lang="en">10.1.16.165,dir_mac_app</value>
</auth.otp.ipAppBinding>
<auth.otp.nasIdAppBinding>
    <value xml:lang="en">10.1.16.165,dir_mac_app</value>
</auth.otp.nasIdAppBinding>
```

Each binding above binds a given IP/nasId to an authentication service ID.

uid

User's Encentuate user name.

appPwd

Application password, which is the password for the above user for the specified application.

save

If set to **false**, this call will return the generated MAC and IMS Server will not save the MAC to its database. The MAC, in this case, will have to be verified by the SOAP client that calls the IMS Server.

If set to **true**, IMS Server will save the MAC to its database and not return the MAC. A SOAP client can make a `verifyOtp` call later to verify the MAC.

channel

Name of the messaging connector that needs to be used to send the MAC. If the channel is specified, the channel is always used, and there will not be any fail-over to the user's preferred channels. However, if the channel is left empty, the user's phone/pager/email will be used according to the user's preference. Fail-over will be provided within these preferences.

msgFormat

The message to be sent to the user. It should follow the format:

```
<message><subject>This is the subject</subject><body>Your MAC  
is: {0}</body></message>
```

where {0} will be replaced by the MAC.

Return value

Returns `ResultMessage`, which consists of `resultCode` and `resultString`.

Returns `nil` for `resultString` if `resultCode` is not **OTP_SUCCESS**.

If `resultCode` is **OTP_SUCCESS**, it returns MAC as `<otp>` (in `resultString`) if `save` is `false`, else MAC is not returned.

Remarks

This operation should be used for requesting MAC from an application logon prompt, where the user provides the application password. This assumes that there is an IMS Connector for the application to allow the IMS Server to verify the application password.

requestOtpWithPasscode

```
public ResultMessage requestOtpWithPasscode(  
    String clientPassword, String idTypeValue, String uid,  
    String passcode, boolean save, String channel, String  
    msgFormat);
```

Synopsis

To request for a MAC from the IMS Server using the user's Encentuate password.

This operation requests the IMS Server to generate a MAC and send it to the user's phone/pager/email according to the user's preference or according to the channel specified in the arguments, after verifying the user's Encentuate password.

Arguments

clientPassword

Shared secret between the SOAP client and IMS Server. It is configured on the IMS Server using the `auth.otp.access_password` key in **ims.xml**, which can be set using the IMS Configuration Utility.

idTypeValue

Specifies the authentication service as configured in the IMS Server. Can be in one of the following 3 formats (in the example below, **"dir_mac_app"** is the authentication service ID):

- `<appldType>IP</appldType> <appldValue>10.1.16.165</appldValue>`
- `<appldType>nasId</appldType> <appldValue>10.1.16.165</appldValue>`
- `<appldType>appName</appldType> <appldValue>dir_mac_app</appldValue>`

For the first two formats, the IP/nasId should be configured in IMS using the appropriate key in **ims.xml**, which can be set using the IMS Configuration Utility (*ActiveCode Deployment >> IP-Application Name Binding* and *ActiveCode Deployment >> NASID-Application Name Binding*):

```
<auth.otp.ipAppBinding>
    <value xml:lang="en">10.1.16.165,dir_mac_app</value>
</auth.otp.ipAppBinding>
<auth.otp.nasIdAppBinding>
    <value xml:lang="en">10.1.16.165,dir_mac_app</value>
</auth.otp.nasIdAppBinding>
```

Each binding above binds a given IP/nasId to an authentication service ID.

uid

User's Encentuate user name.

passcode

User's Encentuate password.

save

If set to **false**, this call will return the MAC generated and IMS Server will not save the MAC to its database. The MAC, in this case, will have to be verified by the SOAP client that makes the call to IMS Server.

If set to **true**, IMS Server will save the MAC to its database and not return the MAC. A SOAP client can make a `verifyOtp` call later to verify the MAC.

channel

Name of the messaging connector that needs to be used to send the MAC. If the channel is specified, the channel is always used, and there will not be any fail-over to the user's preferred channels. However, if the channel is left empty, the user's phone/pager/email will be used according to the user's preference. Fail-over will be provided within these preferences.

msgFormat

The message to be sent to the user. It should follow the format:

```
<message><subject>This is the subject</subject><body>Your MAC
is: {0}</body></message>
```

where {0} will be replaced by the MAC.

Return value

Returns ResultMessage, which consists of resultCode and resultString.

Returns nil for resultString if resultCode is not OTP_SUCCESS.

If resultCode is OTP_SUCCESS, returns MAC as <otp> (in resultString) if save is false, else MAC is not returned.

Remarks

This operation should be used for requesting an MAC from a request MAC Web page, where the user provides the Encentuate password. This assumes that users have already signed up with Encentuate IAM and hence, would have defined their Encentuate passwords.

verifyOtp

```
public int verifyOtp(  
  
    String clientPassword, String idTypeValue, String  
    loginId,  
  
    String keyPasscode, String otp)
```

Synopsis

To verify a MAC for a given user.

This operation requests the IMS Server to verify a MAC for a given user, and return whether it is a valid MAC.

Arguments

clientPassword

Shared secret between the SOAP client and IMS Server. It is configured on the IMS Server using the auth.otp.access_password key in **ims.xml**, which can be set using the IMS Configuration Utility.

idTypeValue

Specifies the authentication service as configured in the IMS Server. Can be in one of the following 3 formats (in the example below, "dir_mac_app" is the authentication service ID):

- <appldType>IP</appldType> <appldValue>10.1.16.165</appldValue>
- <appldType>nasId</appldType> <appldValue>10.1.16.165</appldValue>

- `<appldType>appName</appldType><appldValue>dir_mac_app</appldValue>`

For the first 2 formats, the IP/nasId should be configured in IMS using the appropriate key in **ims.xml**, which can be set using the IMS Configuration Utility (*ActiveCode Deployment >> IP-Application Name Binding* and *ActiveCode Deployment >> NASID-Application Name Binding*):

```
<auth.otp.ipAppBinding>
    <value xml:lang="en">10.1.16.165,dir_mac_app</value>
</auth.otp.ipAppBinding>

<auth.otp.nasIdAppBinding>
    <value xml:lang="en">10.1.16.165,dir_mac_app</value>
</auth.otp.nasIdAppBinding>
```

Each binding above binds a given IP/nasId to an authentication service ID.

loginId

User's Encentuate user name.

keyPasscode

Deprecated parameter. Provide an empty value.

otp

User's MAC that needs to be verified by the IMS Server.

Return value

Returns resultCode.

Enabling MAC authentication for an application using the SOAP API

To enable MAC authentication for an application using the SOAP API:

- ❶ Identify the deployment scenario and customize the application logon interface or provide a request MAC Web page.
- ❷ Develop the SOAP client for the application.
- ❸ Install and configure the IMS Server.

As the following are out of the scope of this document, the reader should refer to a separate deployment guide for Encentuate ActiveCode:

- Configuring the IMS Connector for Mobile Gateway, Communication Server, or Email Server.
- Registering users for MAC.

Deployment scenarios

As described in the this appendix, applications can make use of MAC authentication regardless of whether the logon interface can be customized.

Customizable application logon interface

If the application logon interface is customizable, modify it so that it prompts the user for the following during logon:

- Application user name or Encentuate user name (depends on whether users are expected to have signed up with Encentuate IAM)
- Application password or Encentuate password (depends on whether users are expected to have signed up with Encentuate IAM)
- Selection of preferred channel for MAC to be sent (optional)

After the MAC has been requested, the application logon interface should then perform the following:

- Inform user that the MAC has been sent (or has failed to be sent) as well as the delivery channel
- Ask user for the MAC

Verification of the supplied MAC can be performed by the application via a SOAP call to the IMS Server, or the application's authentication server via SOAP or via RADIUS, with the IMS Server.

Non-customizable Application Logon Interface

If the application logon interface cannot be customized to request for MAC (e.g., a Windows application), a separate request MAC Web page should be provided.

The request MAC Web page should prompt the user for the following during logon:

- Application user name or Encentuate user name (depends on whether users are expected to have signed up with Encentuate IAM)
- Application password or Encentuate password (depends on whether users are expected to have signed up with Encentuate IAM)

- Selection of preferred channel for MAC to be sent (optional)

After the MAC has been requested, the request MAC Web page should then inform user that the MAC has been sent (or has failed to be sent) as well as the delivery channel.

Upon receiving the MAC, the user is expected to launch the application and type in the MAC in the password field of the application logon interface. Verification of the supplied MAC can be performed by the application's authentication server via SOAP or via RADIUS, with the IMS Server.

Developing the SOAP client

Depending on the deployment scenario, the SOAP client may be the application, the request MAC Web page, and/or the application's authentication server.

The SOAP API has been tested on the following platforms:

- Microsoft .NET with Visual Studio .NET
- Apache Axis

Other SOAP client environments can be used as long as they support standard SOAP messages.

SOAP tools consume WSDL to generate SOAP client code. See [WSDL](#) for details.

The WSDL for this API can also be obtained from an installed IMS Server at the following URL ("imsserver" should be replaced by the hostname of your IMS Server).

<https://imsserver/ims/services/encntuate.otp.service.OtpService?wsdl>

Sample code for the following are available in the folders that accompany this document:

- Web application using Visual Basic (web_vb folder)
- Windows application using Visual C# (win_cs folder)
- MAC request Web page using JSP (web_jsp folder)

The high-level steps for enabling MAC authentication for applications using Visual Studio .NET are as follows:

- ❶ Add a Web Reference, pointing it to the WSDL. Name it "Ims".
- ❷ In the appropriate code, create a new `Ims.OtpServiceService` object.
- ❸ When applicable, call the object's methods to request for MAC and verify MAC.

The high-level steps for enabling MAC authentication for applications using Apache Axis are as follows:

- ❶ Use WSDL2Java to automatically create Java stubs and classes.
- ❷ In the appropriate code, create a new `EncentuateOtpServiceOtpServiceSoapBindingStub` object, pointing it to the WSDL.
- ❸ Where applicable, call the object's methods to request for MAC and verify MAC.

IMS Server configuration

- ❶ Add the authentication service of the application using the IMS Configuration Utility (Authentication Services section). Set up the application connector accordingly if the user will use the application password to request for MAC.
- ❷ Set up the following in the ActiveCode Deployment section of the IMS Configuration Utility (**Allowed MAC Client IPs**, **SSL for MAC Client**, **MAC Look-Ahead Number**, **IP-Application Name Binding**, and **NASID-Application Name Binding**):

```
<auth.otp.allowed_client_ips>

<value xml:lang="en">10.1.16.165</value>

<!--IP address of the SOAP client. In this case, the IP address
of the host where the application is configured.-->

</auth.otp.allowed_client_ips>


<auth.otp.ssl_access_only>

<value xml:lang="en">no</value>

<!--Whether SSL access is required.-->

</auth.otp.ssl_access_only>


<auth.otp.verify_ahead>

<value xml:lang="en">25</value>

</auth.otp.verify_ahead>
```

Specify the binding of a SOAP client IP address to an authentication service, using one of the following keys:

```
<auth.otp.ipAppBinding>
```

```
<value xml:lang="en">10.1.16.165,authServiceId</value>
```

```
</auth.otp.ipAppBinding>
```

```
<auth.otp.nasIdAppBinding>
```

```
<value xml:lang="en">10.1.16.165,authServiceId</value>
```

```
</auth.otp.nasIdAppBinding>
```

- ❸ Set up the messaging connectors using the IMS Configuration Utility.
- ❹ Using AccessAdmin (under Authentication service policies section), configure the authentication service to use "MAC" authentication mode.
- ❺ The SOAP client communicates with the IMS Server using one-way SSL. This means that the SOAP client needs to trust the IMS Server's SSL certificate.

If you are deploying the SOAP client on an application server, where there is already a common trust store shared by different applications, you need to import the IMS Server's SSL certificate into the key store as one trusted certification authority entry.

On the Java platform, you can create a key store using the Java key tool utility. On the Visual Studio .NET platform, you can store the IMS Server's SSL certificate in the Windows certificate store using the Certificates snap-in.

You can use Internet Explorer to download the IMS Server's SSL certificate into the Windows certificate store by visiting <https://imsserver/> where "imsserver" is the IMS Server's hostname, and then click on **View Certificate** and proceed to install the certificate in the Local Computer certificate store (*Install Certificate >> Next >> Place all certificates in the following store >> Browse >> Show physical stores >> Trusted Root Certification Authorities >> Local Computer >> OK >> Next >> Finish*).

- ❻ Ensure that the SOAP client (application, request MAC Web page, and/or application's authentication server) specifies the correct authentication service ID or IP address for the caller in the API.

WDSL

The WSDL for the SOAP API can also be obtained from an installed IMS Server at the following URL ("imsserver" should be replaced by the hostname of your IMS Server):

<https://imsserver/ims/services/encentuate.otp.service.OtpService?wsdl>

It is also reproduced here for reference:

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions targetNamespace="https://imssserver/ims/
services/encentuate.otp.service.OtpService" xmlns="http://
schemas.xmlsoap.org/wsdl/" xmlns:apachesoap="http://
xml.apache.org/xml-soap" xmlns:impl="https://imssserver/ims/
services/encentuate.otp.service.OtpService"
xmlns:intf="https://imssserver/ims/services/
encentuate.otp.service.OtpService" xmlns:soapenc="http://
schemas.xmlsoap.org/soap/encoding/"
xmlns:tns1="http://result.ims.encentuate"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:wsdlsoap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:xsd="http://www.w3.org/2001/
XMLSchema"><wsdl:types><schema targetNamespace="http://
result.ims.encentuate"
xmlns="http://www.w3.org/2001/XMLSchema"><import
namespace="http://schemas.xmlsoap.org/soap/encoding/" /
><complexType name="ResultMessage"><sequence><element
name="resultCode" type="xsd:int" /
><element name="resultString" nillable="true"
type="xsd:string" /></sequence></complexType><element
name="ResultMessage" nillable="true"
type="tns1:ResultMessage" /></schema></wsdl:types>

<wsdl:message name="verifyOtpResponse">

  <wsdl:part name="verifyOtpReturn" type="xsd:int"/>

</wsdl:message>

<wsdl:message name="verifyOtpRequest">

  <wsdl:part name="clientPassword" type="xsd:string"/>

  <wsdl:part name="idTypeValue" type="xsd:string"/>

  <wsdl:part name="loginId" type="xsd:string"/>

  <wsdl:part name="keyPasscode" type="xsd:string"/>

  <wsdl:part name="otp" type="xsd:string"/>

</wsdl:message>

<wsdl:message name="requestOtpWithPasscodeRequest">

  <wsdl:part name="clientPassword" type="xsd:string"/>

  <wsdl:part name="idTypeValue" type="xsd:string"/>

  <wsdl:part name="uid" type="xsd:string"/>

  <wsdl:part name="passcode" type="xsd:string"/>

  <wsdl:part name="save" type="xsd:boolean"/>


```

```
<wsdl:part name="channel" type="xsd:string"/>

<wsdl:part name="msgFormat" type="xsd:string"/>

</wsdl:message>

<wsdl:message name="requestOtpResponse">

  <wsdl:part name="requestOtpReturn"
type="tns1:ResultMessage"/>

</wsdl:message>

<wsdl:message name="requestOtpWithPasscodeResponse">
```

Glossary and Abbreviations

AccessAdmin

The management console used by individuals with the Administrator Role and/or the Helpdesk Role to administer IMS Server, and to manage users and policies.

AccessAgent

The client software that manages the user's identity, enabling sign-on/sign-off automation and authentication management.

AccessAssistant

The web-based interface used to provide password self-help for users to obtain the latest credentials to logon to their applications.

AccessProfiles

Short, structured XML files that enable single sign-on/sign-off automation for applications. AccessStudio can be used to generate AccessProfiles.

AccessStudio

The interface used to create AccessProfiles required to support end-point automation, including single sign-on, single sign-off, and customizable audit tracking.

AD

Microsoft Active Directory

ADAM

Active Directory Application Mode

ADSI

Active Directory Service Interfaces

API

Application Programming Interface

application

In AccessStudio, it refers to the system that provides the user interface for reading/entering the authentication credentials.

application group

A set of applications that share the same directory. In other words, a user can logon to any of the applications in the application group using the same user name.

application policy

Collections of policies and attributes governing access to applications.

authentication factor

The different devices, biometrics, or secrets required as credentials for validating digital identities (e.g., passwords, Encentuate USB Key, RFID, biometrics, and one-time password tokens).

authentication service

Verifies the validity of an account; Applications authenticate against their own user store or against a corporate directory.

authorization code

An alphanumeric code generated by an Encentuate Helpdesk user for administrative functions, such as password resets or authentication factors for the Wallet; may be used one or more times based on policy.

biometrics

The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice or handwriting.

CA

Certificate Authority

CAPI

Microsoft Cryptography API

CLT

Command Line Tool

CSN

Card Serial Number (for Mifare RFID cards)

DB

Database

DLL

Dynamic Link Library

DNS

Domain Name Service

EnGINA

Encentuate GINA, which replaces the Microsoft GINA. EnGINA provides a user interface that is tightly integrated with authentication factors and provide password resets and second factor bypass options.

Enterprise Access Security (EAS)

A technology that enables enterprises to simplify, strengthen and track access to digital assets and physical infrastructure.

Enterprise Single Sign-On (ESSO)

A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials (such as a password). Many ESSO products use sign-on automation technologies to achieve SSO—users logon to the sign-on automation system and the system logs on the user to all other applications.

identity wallet

A secured data store for a user's access credentials and related information (including user IDs, passwords, certificates, encryption keys). The Wallet is an identity wallet.

GINA

Graphical Identification and Authentication

GPO

Group Policy Object of Active Directory

HA

High Availability

HMAC

Hashed Message Authentication Code

HOTP

HMAC-based One-Time Password algorithm

ICA

Independent Computing Architecture

ICA Client

Another name for **pnagent.exe** (*Start >> All Programs >> Citrix >> MetaFrame Access Clients >> Program Neighborhood Agent*).

IIS

Microsoft Internet Information Server

IMS Bridge

For extending functionalities of third party programs, allowing them to communicate with IMS Server.

IMS Server

An integrated management system that provides a central point of secure access administration for an enterprise. It enables centralized management of user identities, AccessProfiles, authentication policies, provides loss management, certificate management and audit management for the enterprise.

JMX

Java Management Extensions

LDAP

Lightweight Directory Access Protocol

Mobile Active Code (MAC)

A one-time password that is randomly generated, event-based, and delivered via a secure second channel (e.g., SMS on mobile phones).

MOM

Microsoft Operations Manager.

NLB

Microsoft Network Load Balancer

One-Time Password (OTP)

A one-use password generated for an authentication event (e.g., password reset), sometimes communicated between the client and the server via a secure channel (e.g., mobile phones).

Personal Identification Number (PIN)

A password, typically of digits, entered through a telephone keypad or automatic teller machine.

policy

Governs the operation of Encentuate IAM Enterprise, comprising of two (2) main sets: machine policies (managed through Windows GPO) and IMS-managed policies (managed through AccessAdmin).

Radio Frequency Identification (RFID)

A wireless technology that transmits product serial numbers from tags to a scanner, without human intervention.

RADIUS

Remote Authentication Dial-In User Service

RDP

Remote Desktop Protocol

RDP Client

Another name for **mstsc.exe** (*Start >> All Programs >> Accessories >> Communications >> Remote Desktop Connection*).

register

Signing up for an Encentuate account, and registering a second factor (e.g., USB Key, RFID) with IMS Server.

single sign-on

A capability that allows a user to enter a user ID and password to access multiple applications.

SOAP

Simple Object Access Protocol

SSL

Secure Sockets Layer

USB Key

A portable and personalized device for storing user names, passwords, certificates, encryption keys, and other security credentials.

user name (user ID)

A unique identifier that differentiates the user from all other users in the system.

Wallet

An identity wallet that stores a user's access credentials and related information (including user IDs, passwords, certificates, encryption keys), each acting as the user's personal meta-directory.

